



governmentattic.org

"Rummaging in the government's attic"

Description of document: National Institute of Standards and Technology (NIST) administrative manual and NIST Directives, 2017

Requested date: 15-February-2017

Released date: 06-March-2017

Posted date: 25-June-2018

Source of document: FOIA Request
National Institute of Standards and Technology
FOIA & Privacy Act Officer
100 Bureau Drive, STOP 1710
Gaithersburg, MD 20899-1710
Email: foia@nist.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

MAR 06 2017

This letter serves as the final response to your February 15, 2017, Freedom of Information Act, (FOIA), request to the National Institute of Standards and Technology, (NIST), FOIA #DOC-NIST-2017-000585 - (as amended), in which you requested:

- (1) All segregable portions in a digital/electronic copy of the NIST Administrative manual, including the Table of Contents, which is published on the NIST internal intranet site.
- (2) A digital/electronic copy of all NIST Directives

NIST has completed the actual search for responsive records and enclosed are one hundred and ninety-eight (198) documents consisting of one thousand five hundred seventy-one (1,571) pages that are being released in their entirety.

We hope that this information fully satisfies your request. If you need further assistance or would like to discuss any aspect of your request, you may contact either the analyst who processed your request, FOIA, Mr. Charles Wasil, Management Analyst, at 301-975-4074, or me, the FOIA Public Liaison/Freedom of Information Act Officer, at 301-975-4054. We may also be reached at foia@nist.gov. In addition, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202741-5770; toll free at 1-877-684-6448, or facsimile at 202-741-5769.

You have the right to appeal the response. An appeal must be received within ninety (90) calendar days of the date of this response letter to:

Assistant General Counsel for Litigation, Employment, & Oversight Office
U.S. Department of Commerce, Room 5875
14th and Constitution Avenue N.W.
Washington, D.C. 20230

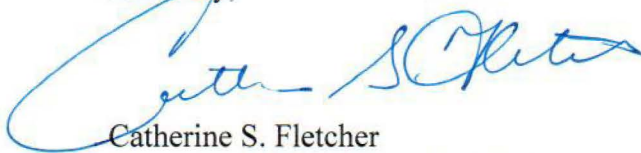
Your appeal may also be sent by e-mail to FOIAAppeals@doc.gov, by facsimile (fax) to 202-482-2552, or by FOIAonline, if you have an account in FOIAonline, at: <https://foiaonline.regulations.gov/foia/action/public/home#>.

The appeal must include a copy of the original request, this response to the request and a statement of the reason for your appeal. The submission (including e-mail, fax, and FOIAonline submissions) is not complete without the required attachments. The appeal letter, the envelope, the e-mail subject line, and the fax cover sheet should be clearly marked "Freedom of Information Act Appeal."

The e-mail, fax machine, FOIAonline, and Office are monitored only on working days during normal business hours (8:30 a.m. to 5:00 p.m., Eastern Time, Monday through Friday). FOIA appeals posted to the e-mail box, fax machine, FOIAonline, or Office after normal business hours will be deemed received on the next normal business day. If the 90th calendar day for submitting an appeal falls on a Saturday, Sunday or legal public holiday, an appeal received by 5:00 p.m., Eastern Standard Time, the next business day will be deemed timely. If the 90th calendar day for submitting an appeal falls on a Saturday, Sunday or legal public holiday, an appeal received by 5:00 p.m., Eastern Time, the next business day will be deemed timely.

It was previously determined that you are in the "all other" requester category for which chargeable services include search and duplication of responsive documents excluding the cost of the first 2 hours of search and the first 100 pages of duplication. The search and duplication costs were under the chargeable threshold; thus, the documents are being provided at no cost.

Sincerely,



Catherine S. Fletcher
Freedom of Information Act Officer

Enclosure(s)

Admin Manual TOC
Admin Manual PDF
NIST Directives Inventory
Directories PDF

Administrative Manual Table of Contents

Subchapter	Content Owner	Effective Date
ADMINISTRATION AND MANAGEMENT		
2.03 Acquisition	OAAM	6/21/2006
2.04 Storeroom Services	OFPM	10/30/2009
2.06 Records Management	M&O	7/18/2005
2.08 Government Motor Vehicle Operator Identification	OFPM	2/9/1996
2.12 Auditoriums and Conference Rooms	PAO	10/1/2009
COMMITTEES		
3.02 Membership in Standards Bodies and Professional Organizations This link is only for Professional Organization Membership, section 3.02.09	SCO	7/11/2011
COMMUNICATIONS		
4.04 Telecommunications Services	CIO	2/1/2010
4.05 Correspondence	COS	9/24/2009
TECHNOLOGY SUPPORT		
5.01 Use of Designated NIST Facilities for Proprietary and Non-Proprietary Measurements	TPO	2/1/2008
5.03 Use of NIST Name in Advertising	PAO	6/30/2009
5.04 Non-Reimbursable Technical Assistance by NIST	TPO	3/26/1997
5.06 Protecting the Confidentiality of Proprietary Information Received by NIST	TPO	5/15/1997
5.07 Treatment of NIST's Proprietary Information	TPO	5/15/1997
5.08 NIST Cooperative Research and Development Agreement Program	TPO	4/14/1998
5.09 Inventions and Patents	TPO	1/11/2007
5.10 Licensing NIST Inventions	TPO	4/5/2006
5.12 Contract Research Performed by NIST for Non-Federal Parties	Budget	11/10/1997
5.16 Traceability	MML	8/12/2009
5.22 NIST Trademark Protection	TPO	6/4/2008
EMERGENCY OPERATIONS		
6.01 Procedures for NIST Employees in a National Emergency	ESO	6/30/2009
6.05 Fire Protection Program	ESO	8/31/2009
6.06 Facility Shutdown Due to Lapse of Appropriations	ADMR	11/20/87
6.07 Building 101 Corridor Utilization Policy	OFPM	4/30/2009
EQUIPMENT AND FACILITIES		
7.02 Maintenance, Modifications, Improvements, and Replacement - Facilities Management	OFPM	11/21/2001
7.04 Building Designations	OFPM	11/21/2001
7.07 Use of Grounds and Outdoor Facilities	OFPM	8/31/2009
7.09 Precious Metals	OFPM	2/3/2009
FINANCIAL MANAGEMENT		
8.01 Structure and Responsibilities	Budget	6/22/2000
8.02 Fund Structure	Budget	9/10/2009
8.03 Budget Formulation	Budget	6/4/2008
8.04 Appropriated Funds	Budget	9/8/2006
8.09 Official Entertainment	CFO	8/24/2000
8.10 Gifts and Bequests	CFO	3/10/2011

Administrative Manual Table of Contents

Subchapter	Content Owner	Effective Date
8.11 Equipment Financing	Finance	8/11/2009
8.12 Official Travel	Finance	10/29/2009
OFFICE OF WORKFORCE MANAGEMENT		
10.01 Hours of Duty and Leave Administration	OHRM	9/10/2004
10.08 Training	OHRM	5/20/2005
10.17 Time and Attendance	OHRM	8/5/2009
SAFETY		
12.03 Ionizing Radiation	OSHE	8/17/2010
SPECIAL PROGRAM ACTIVITIES		
14.02 Animal Care and Use	HSPO	10/20/1995
14.05 Standard Reference Data Program	TS	8/27/2001

STOREROOM SERVICES

Sections

2.04.01 Purpose

2.04.02 Scope

2.04.03 Legal Authority

2.04.04 Policy

2.04.05 Delegation of Authority

2.04.06 Responsibilities

2.04.07 Storeroom Operation

2.04.08 Storeroom Commodity Committees

2.04.09 Stocked Compressed Gases and Liquids

2.04.10 Non-Stock Compressed Gases and Liquids (Special Order)

2.04.11 Content Owner

2.04.12 Effective Date

2.04.01

PURPOSE

This subchapter describes services, supplies, and equipment provided by the NIST-Gaithersburg storerooms.

2.04.02

SCOPE

The provisions of this subchapter apply to NIST-Gaithersburg. Information on the NOAA Corporate Finance and Administrative Services Offices operated storerooms for NIST-Boulder is available at the following website: <http://www.masc.noaa.gov/>.

2.04.03

LEGAL AUTHORITY

41 CFR Chapter 101, Federal Property Management Regulations, Subchapter E, Supply and Procurement, specifies the criteria used in determining which items are stocked in the storerooms.

2.04.04

POLICY

The Logistics Group, of the Chief Facilities Management Officer's Administrative Services Division, orders and stocks supplies in central Storerooms for which there are recurring demands. Criteria considered when determining whether to stock a supply in the central Storerooms include demand or rate of use, shelf life, and price advantage. The Building 301 Storeroom is the main store containing the vast majority of stock items. The Building 304 Storeroom is specifically stocked for metals and is maintained by the Fabrication Technology Division.

2.04.05

DELEGATION OF AUTHORITY

Authority to operate the NIST storerooms has been delegated to the Chief, Administrative Services Division, who has further delegated the management to the Logistics Supply Management Officer. This authority includes the receipt and acceptance of stock, authorization of payments, establishment of appropriate inventory management records, and stocking, issuing, performing physical inventories, deleting, and requisitioning the replenishment of stock.

2.04.06

RESPONSIBILITIES

a. The Office of the Chief Facilities Management Officer's Administrative Services Division Logistics Group is responsible for operation of the main storeroom in Building 301 at Gaithersburg, Maryland. Responsibilities include:

- (1) Stock a wide variety of items in the following commodities: electronics, tools and hardware, electrical, plumbing, metals and chemistry items, office supplies, building materials, compressed gases, and safety items;
- (2) Provide service to storeroom patrons by answering questions, giving direction to find items, efficiently scanning each item purchased, and assist with packaging for delivery or carrying by the customer;
- (3) Promptly answer all telephone inquiries within 4 hours;
- (4) Monitor and fill all online and mail orders for stock items within 2 days of receipt; and
- (5) Meet quarterly with storeroom commodity committees to discuss customer suggestions, concerns and problems with storeroom items including new, current, and/or deleted.

b. The Fabrication Technology Division is responsible for operation of the metals storeroom in Building 304 at Gaithersburg, Maryland. Responsibilities include:

- (1) Stock a variety of metals and plastics;
- (2) Provide requested service while the customer waits, unless volume of the order is excessive; and
- (3) Provide advice and assistance about the various metals and plastics stocked.

c. Participating employees are responsible for:

- (1) Providing the correct project and task number at the time of purchase, obtained from their division's Administrative Officer; and
- (2) Ensuring items purchased are only used for professional duties while at NIST.

d. Administrative Officers (AOs) are responsible for:

- (1) Providing, upon request, project-task information and authorization for payment to the Administrative Services Division for items purchased by employees of their division;
- (2) Providing the correct project-task to the division's employees to be used in the Storeroom for purchases;
- (3) Approving payment for cylinder rental on a monthly or quarterly basis; and
- (4) Receiving copy number two (2) of cylinder purchase orders and notifying the end user that it has arrived.

e. See section 2.04.08 of this subchapter for responsibilities of the Commodity Committees.

2.04.07

STOREROOM OPERATION

To meet the various demands of the NIST staff, the Administrative Services Division, Logistics Group operates the Main Storeroom in Building 301 and the Fabrication Technology Division operates a metals storeroom located in Building 304 at Gaithersburg. Storeroom Hours are Monday – Friday 7:30am to 4:00pm (Closed daily from 12 to 1pm)

a. Building 301 Self-Service Main Storeroom - Customers are free to walk through the self-service Main Storeroom and select items for purchase. The customer brings the selected items to the checkout counter and provides the storekeeper with their name, division and group number, the project task number and work order numbers (when applicable). Administrative Officers can monitor Storeroom purchases through an online

database available at the following address
<https://webapp01.nist.gov:7333/maxissues/searchIssuesForm.jsp>.

(1) On-Line, and Mail Orders – All on-line and mail orders are filled at the Building 301 Main Storeroom and delivered to the delivery point listed. Cryogenic liquids, compressed gases, and hazardous material orders will not be filled online or through mail. Refer to paragraphs i. and ii. of this section for instructions on ordering.

(i) On-Line Orders - Customers may submit orders on-line using the Storeroom Catalog.

(ii) Mail Orders - Customers may send Form NIST-293, Storeroom Requisition, to the Logistics Group, Mail Stop 1922, to request delivery of stocked items. Form NIST-293 must include stock number(s), item(s) description, quantity ordered, project task, and delivery information (name, division/group, building, telephone and room number).

(2) Return of Storeroom Items – Customers may return unneeded items, purchased from the Building 301 Main Storeroom only, within 30 days of purchase, providing they can give the purchaser's name, date of purchase, and if the item is in new/resalable condition. Credits will be issued using the Maximo storeroom system, no paper invoice will be provided. The Administrative Officer may request verification on Storeroom discrepancies within 45 days of a charge or credit.

b. Metals Storeroom (Building 304) -- The Metals Storeroom stocks a variety of metals and plastics. This is not a self-service storeroom; customers must complete Form NIST-293 to purchase stocked items. Customers must provide a project task, work order number (as applicable), stock number, and dimensions as required on Form NIST-293. Except for unusually large orders, this service is provided while the customer waits. Storeroom staff are available to provide advice and assistance about the various metals and plastics stocked. Credits will not be issued for special items or cuts. All sales are final.

2.04.08

STOREROOM COMMODITY COMMITTEES

a. Staff from the Logistics Group, Administrative Services Division, meet regularly with storeroom customers to discuss customer suggestions, concerns and problems with new, current, and deleted storeroom items. Interested NIST employees may assist the staff of the Logistics Group in evaluating stocked items for specific purposes. The Logistics Group establishes Commodity Committee panels annually for the following commodities: electronics, tools and hardware, electrical, plumbing, building materials and metals, safety and office supplies. A memorandum or e-mail indicating interest in participating on a panel may be sent to the Logistics Group. Commodity Committee meetings meet at least twice a year, but no more than quarterly.

b. A catalog of items maintained in the NIST storerooms

c. An employee or organizational unit may recommend that a new item be added to the storeroom by submitting Form NIST-42, Suggestion for New Item in Storeroom. Each request for a new item is evaluated in accordance with the criteria referenced in Section 2.04.03.

2.04.09

STOCKED COMPRESSED GASES AND LIQUIDS

The Logistics Group, Administrative Services Division, maintains a stock supply and delivery program for liquid nitrogen using dewars and certain compressed gases using cylinders. Customers placing orders or needing regular and reoccurring deliveries, may make arrangements by contacting the Building 301 Main Storeroom on extension 6052.

- a. Dewars to be filled should be empty prior to pick-up.
- b. Upon return, dewars are inspected for safe use and operation. Those failing inspection will be immediately returned to the owning Organizational Unit for repair.
- c. Dewars will be filled and returned within 3 days of pick-up. Dewars larger than 240 liters will not be filled due to safety concerns.
- d. Logistics Group Warehouse staff deliver full cylinders of compressed gases to the loading dock of each building per customer order. The user is responsible for transporting the cylinder safely to their laboratory.
- e. NIST-stocked cylinders may be stored in the loading dock for no more than 15 days. Any cylinder in the loading dock longer than 15 days will be returned to the storeroom, and the customer will not be credited.
- f. Dewars over 100 liters will be filled at the tank in the basement of Building 215.
- g. Dewars of 25, 50, or 100 liters of liquid Nitrogen will be filled in Building 301 and delivered to the laboratory that placed the order.
- h. The division that placed the order will be charged labor associated with filling and special delivery of liquid Nitrogen to their laboratories.
- i. Regardless of the dewer size, all orders for liquid Nitrogen must be placed with the 301 Storeroom by calling extension 6052.

2.04.10

NON-STOCKED COMPRESSED GASES AND LIQUIDS (SPECIAL ORDER)

- a. Orders for special cylinders placed through the Acquisition Management Division are received, recorded and then delivered by the Administrative Services Division's Logistics Group staff to building loading docks.

- b. Helium orders must be placed through the Logistics Group at extension 6052 by 11:30am on Monday and/or Wednesday for next day delivery. Orders for next-day delivery not placed within these timeframes cannot be guaranteed for next-day delivery, and, if delivered, the contractor may impose additional charges that must be paid by the customer. Dewars for Helium are available from the contractor in 30, 60, 100, and 250 liters.
- c. Cylinders can only be delivered if storage rack areas are available in order to secure the cylinders safely. Customers should ensure that cylinders are claimed within thirty (30) days, or place a note with a current date or a note indicating the date by when the cylinder will be used in order to justify continued storage. These additional storage days should not exceed the total of sixty (60) days in approved storage space on the building loading dock.
- d. Cylinders and dewars carry a rental/demurrage charge for late return past the agreed contract period. Cylinder demurrage charges are sent to each division's Administrative Officer on a monthly or quarterly basis. Divisions that are unable to locate their cylinders are responsible for replacement charges. In order to minimize these charges, it is important that organizational units track the cylinders in their possession and that they return them to the loading dock/receiving areas' cylinder rack, in the racks marked empty for return, as soon as they are empty and no longer needed. This will allow the Logistics Group to make arrangements to have them returned to the contractor to avoid demurrage or rental charges being incurred. Customers must secure empty cylinders in the racks properly, ensuring that valves are closed and caps are properly affixed.
- e. In most cases, gases requiring special handling and customer signature, because of their high toxicity or other special characteristics, will be delivered by the outside contractor directly to the customer (end user). If these cylinders are only partially used and/or require special handling when the end user is finished using them, the end user must contact the Building 301 Main Storeroom (x6052) to make arrangements for pick up.

2.04.11

CONTENT OWNER

Chief Facilities Management Officer

Chief, Administrative Services Division

Supply Management Officer, Logistics Group

2.04.12

EFFECTIVE DATE

October 30, 2009

RECORDS MANAGEMENT

(Administrative and Technical)

Sections

2.06.01 Purpose

2.06.02 Scope

2.06.03 Policy

2.06.04 Definitions

2.06.05 Responsibilities

2.06.06 Files Management

2.06.07 Filing Systems

2.06.08 Removal of Papers

2.06.09 Records Holding Area

2.06.10 Managing Electronic Records

Appendix A - Retirement (Transfer) of NIST Records

Appendix B - Recalling Retired Records

Appendix C - Disposition of NIST Test Folders and Test Reports

Appendix D - Disposition of Papers Covered by the Privacy Act of 1974

Appendix E - Disposition of Records by Departing Employees

2.06.01

PURPOSE

This subchapter prescribes policies, responsibilities, and procedures for the management of records and certain nonrecord reference material at the National Institute of Standards and Technology (NIST). Instructions for the management of classified records are outlined in Subchapter 13.01.

2.06.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder and covers administrative and

technical files, file material, records, nonrecord material, and research notebooks and technical journals.

2.06.03

POLICY

a. It is NIST policy to ensure that all administrative and technical records, including those in electronic form, contain adequate and proper information on the functions, organization, policies, procedures, decisions, scientific and technical progress, and essential transactions they are intended to document; are sufficient to protect the legal and financial rights of the government and of persons directly affected by NIST actions; are easily retrievable and usable; are protected from unauthorized access to, or loss, removal, or theft of; are protected from unauthorized disclosure; and are disposed of only in compliance with approved NIST Records Schedules and General Records Schedules.

b. It is NIST policy that all NIST employees engaged in research and development activities maintain a thorough and accurate record of their work by keeping a research notebook following internal Operating Unit policies. Employees conducting research using electronic media shall maintain a notebook that chronologically documents the progress of their research and indexes electronic work files so that primary experimental results may be retrieved.

c. Records at NIST are to be managed in an economical and efficient manner, in accordance with the objectives of the Federal Records Act of 1950 as amended by the Federal Records Management Amendments of 1976 (44 U.S.C. 2901 et. seq.) and instructions given in Department Administrative Order (DAO) 205-1. In compliance with the provisions of the disposal of records chapter of Title 44 in the United States Code (44 U.S.C. 3301 et. seq.), records of continuing value will be preserved and records of insufficient value to warrant further attention will be destroyed.

d. Official record files are the property of the government, not the property of individual employees. All technical records, including research notebooks, journals, electronic records, data, calculations, etc., pertaining to NIST activities are official files of the government and, as such, are the property of the government, not the employee. These records are not to be removed from NIST without the proper authority. This applies when an employee transfers, retires, or otherwise separates from NIST.

2.06.04

DEFINITIONS

a. Audiovisual Records - Include program and information motion pictures, still pictures, sound records, video recordings, and related documentation. For purposes of records management, these records include the management of audiovisual records and related records that document the creation and/or acquisition of audiovisual records and were created for or used in the retrieval of information about or from audiovisual records.

b. Blowback - An enlargement of a micro-image to full readable size on a viewer or on printed paper.

- c. Disposal List - Serves as a one-time authorization permitting the disposal of a specific group of records which is no longer needed. After approval by the appropriate organizational unit, records which have reached their authorized disposal date are destroyed.
- d. Disposition - A plan for the future of records, i.e., a determination of how long materials should be retained in office space and/or in the NIST Records Holding Area or Federal Records Centers.
- e. Electronic Recordkeeping - Procedures and systems for creating, using, maintaining, transmitting, and disposing of records in electronic form.
- f. Electronic Filing - Transmittal and entry into an electronic system of records or information received from the public or other sources outside NIST, e.g., the electronic filing of patent and trademark applications and related information.
- g. File Copies - Filed in a central file and/or other officially prescribed file for the continuing or permanent use and reference of an agency or office thereof. Generally, file copies do not refer to extra copies made for convenience purposes by those individuals who deal with a particular document.
- h. Electronic Recordkeeping System - An electronic information system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition (36 CFR 1234.2) while ensuring that the records it maintains will have sufficient authenticity and reliability to meet NIST's recordkeeping needs.
- i. Records Management Application - Software that manages records. Its primary management functions are categorizing and locating records and identifying records that are due for disposition. Records Management Application software also stores, retrieves, and disposes of the electronic records that are maintained in its repository. The National Archives and Records Administration (NARA) recommends that agencies use DoD 5015.2-STD *Design Criteria Standard for Electronic Records Management Software Applications* and the DoD-certified products as a baseline when selecting a Records Management Application to manage agency's electronic records.
- j. Hardcopy - Written or printed information on paper.
- k. Microform - A medium containing microimages, such as microfilm, microfiche, microthin jackets, aperture cards, and computer output microfilm.
- l. Micrographics - The science and technology of document and information microfilming and associated microform systems.
- m. Nonrecord Material - Consists of extra copies of documents preserved for convenience of reference, stocks of processed documents, preliminary work sheets, and similar papers that need not be made a matter of record, and which ordinarily are not to be incorporated into the official files.

n. Office of Record - Has primary responsibility for the subject area and for the filing and disposition of the record copy of a document.

o. Official File - Documents policy, procedural, organizational, and reportorial activities of NIST; the file consists of incoming correspondence, all background material, and the yellow "Official File Copy" tissue. Official files will be retired to the NIST Records Holding Area or Federal Records Centers.

p. Official Materials - Made, received, or obtained in connection with the transaction of public business or official duties and responsibilities.

These materials, whatever their nature, belong to the government and not to an employee because they were prepared, reviewed, or obtained (including extra copies) with government funds and/or on government time. Correspondence, or portions thereof, designated "personal," "private," "confidential," etc., relevant to the conduct of public business are considered official material. Notes or transcriptions of official meetings and telephone conversations involving official business, drafts, speeches, extra copies of papers, official permits, reference materials collected to assist the employee in their work, etc., are all official materials. Some official materials may not be removed; others may be removed under certain conditions as indicated in Appendix E.

q. Personal Papers - Private or nonofficial papers pertaining only to an individual's personal affairs and kept in the office of a federal official. They will be clearly identified by that person as nonofficial and will at all times be filed separately from the official records of the office. In cases where matters requiring the transaction of official business are received in private personal correspondence, the portion of such correspondence pertaining to official business will be extracted and made a part of the official files.

r. Records - Books, papers, maps, photographs, research notebooks/technical journals, data, electronic records, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them (44 U.S.C. 3301).

(1) Current Records - Records necessary to conduct the current business of an office and therefore generally maintained in office space and equipment.

(2) Semi current Records - Records required so seldom to conduct agency business that they should be moved to a Records Holding Area or directly to a Federal Records Center.

(3) Noncurrent Records - Records no longer required to conduct agency business and therefore ready for authorized disposition.

(4) Permanent Records - Records considered to be unique or valuable in documenting the history of an agency, or for other reasons, and are to be preserved as part of the National Archives of the United States.

(5) Electronic Records - Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 U.S.C. 3301 (36 CFR 1234.2).

s. Research Notebook - A hard covered or spiral bound notebook with pre-printed, sequentially numbered pages, such as the types available from the NIST storeroom. Research records must be permanent, contemporaneous with the research, accurate, and reasonably protected from compromise. Electronic "notebooks" are allowable at the discretion of the OU.

t. Schedules - General Records Schedules, published by the NARA, govern the disposition of records common to all or several agencies. In 1978, use of the General Records Schedules was made legally mandatory [Title 44 U.S.C. 3303a(b)]. NIST records not common to all agencies are covered by the NIST Records Schedules drafted by the NIST Records Management Officer and approved by NARA.

2.06.05

RESPONSIBILITIES

a. The NIST Records Management Officer, Management and Organization Division, administers the Records Management Program at NIST.

(At Boulder, a staff member of the Engineering, Maintenance and Support Services Division serves as NIST-Boulder Records Liaison, under the guidance of the NIST Records Management Officer.)

The NIST Records Management Officer is responsible for:

- (1) Maintaining an effective Records Management Program;
- (2) Ensuring NIST compliance with the provisions of Department Administrative Orders and all other records management policies;
- (3) Assisting organizational units in planning their records management programs;
- (4) Advising on equipment and methods of maintaining useful records;
- (5) Destroying papers covered by the Privacy Act of 1974 (see Appendix D);
- (6) Implementing policies and procedures to ensure the proper disposition of all records regardless of physical form or characteristics including paper, micrographic, audiovisual, and/or electronic records;
- (7) Developing, updating, and maintaining records schedules;

(8) Providing storage and retrieval service for noncurrent records and for classified records (both current and noncurrent);

(9) Arranging training for NIST employees in sound and efficient filing and records disposal practices; and

(10) Acting as liaison with the Department of Commerce Records Management Officer in matters that relate to the management and disposition of NIST records.

b. Division chiefs and higher officials are responsible for:

(1) Authorizing the destruction of records in accordance with the schedules governing the disposal of the records (This authority may not be redelegated.);

(2) The proper and adequate documentation of programs, policies, procedures, and accomplishments; and for the maintenance of systematic files;

(3) Ensuring that the technical activities of their staff are fully documented, that appropriate control measures are in place so that either paper or electronic records are retrievable, and that all staff engaged in research are properly instructed; and

(4) Ensuring that technical records are not removed from NIST without proper authority even when an employee transfers, retires, or otherwise separates from NIST. NIST laboratories that conduct research predominately using electronic media may be allowed to implement procedures that accomplish the same policy goals stated in paragraph 2.06.03b, but use alternatives to bound notebooks.

c. NIST supervisors are responsible for ensuring that all employees under their supervision are instructed on the proper procedures for maintaining records.

d. Organizational units having primary responsibility for a subject area are responsible for:

(1) Maintaining the official file copy;

(2) Providing background material upon request; and

(3) Disposing of the file when appropriate.

e. Records Liaisons assist the NIST Records Management Officer, by overseeing:

(1) Organization, maintenance, and use of records in their organizational units (files management); and

(2) Systematic disposal of these records (records scheduling and disposition).

f. NIST employees share responsibility for the adequate and proper documentation of NIST's administrative and technical operations.

NIST employees engaged in research and development activities are responsible for:

(1) Maintaining a thorough and accurate record of their work by keeping a research notebook (See Section 2.06.04s for information regarding research notebooks.);

(2) Following recordkeeping procedures outlined in Subchapter 5.09 when intellectual property issues, such as patents, copyrights, etc., are likely to be important since these records establish the legal foundation for future claims; and

(3) When using electronic media, maintaining a research notebook that chronologically documents the progress of their research and indexes electronic work files so that primary experimental results may be retrieved.

2.06.06

FILES MANAGEMENT

a. It is NIST policy to keep files to a minimum and automate where possible.

b. Files are maintained on a decentralized basis. However, when a function is more efficiently served on a centralized basis, a central file for that function may be established.

c. NIST utilizes the NARA Records Management Website as a reference and guide to filing operations. The following website is incorporated by reference into this subchapter:
http://www.archives.gov/records_management/index.html.

d. Records Management (at Boulder, the Engineering, Maintenance and Support Services Division) gives advice and guidance on filing systems and files management.

2.06.07

FILING SYSTEMS

a. Alphabetic and numeric filing are basic methods used to manage record material. In general, records at NIST are filed alphabetically by subject or name, with alphabetic or numeric breakdowns within the general subject headings, as needed. Straight numeric filing may be appropriate in some instances.

b. Division chiefs or higher officials determine the method appropriate to their needs and are authorized to establish Official File Stations.

c. In addition to general files, chronological or reading files, and follow-up files are authorized for use at NIST. The chronological file consists of copies of outgoing correspondence, arranged by date. The follow-up file is a convenience file, centrally maintained, to ensure that deadlines or action dates are met.

2.06.08

REMOVAL OF PAPERS

a. There are criminal sanctions against the unlawful removal or destruction of records, documents, papers, and other property held by federal agencies. These sanctions are directed in part to keep federal officers and employees from disposing of official materials in their possession or control, thereby depriving the government of their usefulness in conducting its affairs. The efficiency, continuity, and consistency of many governmental activities depend increasingly on the existence and availability of complete information concerning previous official actions and experience. The removal or destruction of official nonrecord materials by a departing employee may impose substantial handicaps to the efficient functioning of an employee's successors. Much of the information a departing employee receives, the information they prepare, the actions they take, and the materials they accumulate are in response or related to requests for advice or services they have performed in connection with their official duties and responsibilities. Accordingly, materials that would deprive the Department, or an office thereof, of such documents or papers, or diminish its effectiveness or efficient functioning are to be retained in that office.

b. It is Departmental policy to permit departing employees to retain or discard nonrecord official materials which they have accumulated, with certain exceptions, subject to the guidelines outlined in Appendix E of this subchapter. It is also Departmental policy to permit an employee to make an extra copy of materials which they desire to take with them provided that such materials are not restricted in their removal from the Department. Because the employee will be using government facilities, materials, and other employee assistance, normal administrative economies are to be exercised in this respect.

c. Original records must not be removed from NIST control. Any NIST employee who contemplates the removal of papers for the purpose of loaning or gifting them to anyone outside NIST who has requested them, must consult with Records Management for instructions. Usually, if the records requested are not confidential or classified, the division chief having custody may authorize the release of copies of originals, advising Records Management of this action.

d. Donation of Temporary Records - When the public interest will be served, a federal agency may propose the transfer of records eligible for disposal (destruction) to an appropriate person, organization, institution, corporation, or government that has requested them. Records will not be transferred without prior written approval by the NIST Records Management Officer and the National Archives and Records Administration. To request donation, send a memorandum to the NIST Records Management Officer stating:

(1) The name of the department or agency, and subdivisions thereof, having custody of the records;

(2) The name and address of the proposed recipient of the records;

(3) A list containing:

- (a) An identification by series or system of the records to be transferred,
- (b) The inclusive dates of the records, and
- (c) The NARA disposition of job (SF-115) or GRS and item numbers that authorize disposal of the records;
- (4) A statement providing evidence:
 - (a) That the proposed transfer is in the best interest of the government,
 - (b) That the proposed recipient agrees not to sell the records as records or documents, and
 - (c) That the transfer will be made without cost to the government;
- (5) A certification that:
 - (a) The records contain no information the disclosure of which is prohibited by law or contrary to the public interest, and/or
 - (b) That records proposed for transfer to a person or commercial business are directly pertinent to the custody or operations of properties acquired from the government, and/or
 - (c) That a foreign government desiring the records has an official interest in them.

NARA will consider such request and determine whether the donation is in the public interest. Upon approval NARA will notify the requesting agency's Records Management Officer in writing. If NARA determines such a proposed donation is contrary to the public interest, the request will be denied and the agency's Record Management Officer will be notified that the records must be destroyed in accordance with the appropriate disposal authority.

e. Loan of Permanent and Unscheduled Records - The Archivist of the United States has authority over the placement of permanent records (44 U.S.C. 2107 and 2904). (Unscheduled records are treated as permanent records). No permanent or unscheduled records shall be loaned to nonfederal recipients without prior written approval by the NIST Records Management Officer and the National Archives and Records Administration. To request loan of permanent or unscheduled records, send a memorandum to the NIST Records Management Officer stating:

- (1) The name of the department or agency and subdivisions thereof, having custody of the records;
- (2) The name and address of the proposed recipient of the records;
- (3) A list containing:
 - (a) An identification by series or system of the records to be loaned,

- (b) The inclusive dates of each series, and
 - (c) The NARA disposition job (SF-115) and item numbers covering the records, if any;
 - (4) A statement of the purpose and duration of the loan;
 - (5) A statement specifying any restrictions on the use of the records and how these restrictions will be administered by the donee; and
 - (6) A certification that the records will be stored according to the environmental specifications for archival records.
- f. No material, even though judged not to be records within the meaning of the disposal of records chapter of Title 44 in the U.S. Code, shall be withdrawn if its withdrawal will create such a gap in the files as to disrupt the proper documentation of NIST activities.
- g. When employees transfer, retire, or otherwise separate from NIST, their collections are reviewed by the separating employee, the Records Liaison, and NIST Records Management Officer (at Boulder, the Engineering, Maintenance and Support Services Division). If the separating employee cannot be present, the division chief names a suitable replacement for review. The purpose of this review is to:
- (1) Identify, select, and preserve those parts of the collections which may have continuing value to NIST; and
 - (2) Identify and ensure the proper disposition of any official record material and nonrecord material of no value.

Departing employees also refer to Appendix E.

2.06.09

RECORDS HOLDING AREA

- a. At Gaithersburg, Records Management maintains a Records Holding Area in Building 101, Room C29, for storing noncurrent records. Records retention schedules are applied by records management before records are accepted for storage in accordance with the General Records Schedules or NIST Records Schedules for each type of record. Records are stored in the NIST Records Holding Area or transferred to the Federal Records Centers (Suitland, MD or St. Louis, MO). After a given period of time, temporary records are destroyed (with the concurrence of the organizational unit); permanent records are transferred to the National Archives.
- b. Stored records may be recalled by NIST employees when needed. Contacts with the Federal Records Centers or the National Archives MUST BE through NIST Records Management.

2.06.10

MANAGING ELECTRONIC RECORDS

Records and information in electronic form are managed in conformance with policies

established by the National Archives to ensure the effective and efficient management of electronic records throughout their life cycle from creation to final disposition; to preserve records needed for fiscal, legal, administrative, or historical purposes; to destroy in a timely manner information no longer needed; to ensure cost effective use of automated data processing equipment, storage media, and other resources; and to facilitate retrieval of electronically stored records. General Records Schedules (GRS) and NIST Electronic Records Schedules provide disposal authorization for certain electronic records and specified hard-copy (paper) or microform records that are integrally related to the electronic records. They apply to disposable electronic records created or received by Federal agencies including those managed for agencies by contractors. They cover records created by computer operators, programmers, analysts, systems administrators, and all personnel with access to a computer. Disposition authority is provided for certain master files, including some tables that are components of database management systems, and certain files created from master files for specific purposes. In addition, these schedules cover certain disposable electronic records produced by end users in office automation applications. Electronic records not covered by GRS or NIST Electronic Records Schedules may not be destroyed unless authorized by a Standard Form 115 that has been approved by the NARA.

APPENDIX A

RETIREMENT (TRANSFER) OF NIST RECORDS

Records may be retired (transferred) to the NIST Records Holding Area, the Federal Records Centers, or the National Archives. Before retiring or transferring records, contact Records Management, Management and Organization Division (at Boulder, the Engineering, Maintenance and Support Services Division).

1. Retirement (Transfer) of Records

a. Standard 15" x 12" x 10" records storage boxes are available from Records Management, (at Boulder, the Storeroom). These boxes are to be used only for storage of records in the NIST Records Holding Area, or for transfer of records to the Federal Records Centers. Consult Records Management before attempting to store any oversized or undersized records, ledgers, drawings, etc., as only NARA-approved containers will be accepted for storage. To estimate the number of containers needed for regular-size records, calculate as follows: one letter-size file drawer fills one and one-half record boxes as each box holds one cubic foot of material.

b. A detailed description of the contents of each box is necessary. This inventory must be typed on the Form NIST-1153, Records Transmittal and Receipt.

(At Boulder, this inventory must be typed on Form SF-135, Records Transmittal and Receipt, which may be obtained from the Engineering, Maintenance and Support Services Division. Call the Engineering, Maintenance and Support Services Division, for records transfer to the Denver Federal Records Center and/or Denver Archives.)

c. Follow the Instructions for Retiring Records

Nonrecord material MAY NOT be stored in the NIST Records Holding Area or the Federal Records Centers. Questions concerning whether the files are record or nonrecord should be directed to Records Management. (At Boulder, call the Engineering, Maintenance and Support Services Division.)

Records, record boxes, and Records Transmittal and Receipts prepared incorrectly will be returned to the originating organizational unit for correction.

2. Transfer to the National Archives - Permanent records are offered to the Archivist of the United States by the NIST Records Management Officer. If the material is acceptable as worthy of permanent preservation, Records Management arranges for the transfer of the records. An Accession Inventory is prepared by the National Archives which, when signed by an agent from each of the agencies, constitutes formal transfer of custody from NIST to the National Archives. Records so transferred remain available for loan to NIST by contacting Records Management. They are also available for research purposes at the National Archives. (At Boulder, initial

contact should be made with the Engineering, Maintenance and Support Services Division which handles arrangements with Records Management.)

3. Restrictions on the Use of Transferred Records - When records transferred from the custody of organizational units at NIST to the custody of Records Management, the National Archives or Federal Records Centers, restrictions with respect to access or use are maintained. Restrictions may be removed only upon approval by NIST.

APPENDIX B

RECALLING RETIRED RECORDS

1. Recalling Records

a. An organizational unit may request the recall of records in the custody of Records Management, Management and Organization Division, in the NIST Records Holding Area, Federal Records Centers, or the National Archives by calling Records Management. Please be prepared to furnish:

- (1) Accession number or the NIST Records Holding Area shelf number;
- (2) Box number; and
- (3) Item requested.

b. Delivery of records from the NIST Records Holding Area or Federal Records Centers to NIST organizational units are arranged by Records Management.

c. Visits by NIST employees to the NIST Records Holding Area to examine or search records specifically needed are by appointment. Call Records Management to arrange for an appointment. Approval to examine or search records not created by an employee's own organizational unit must be approved in writing by the creating organizational unit before arranging an appointment. The request to examine or search another organizational unit's records must include:

- (1) List of records to be examined or searched;
- (2) Shelf or accession number;
- (3) Box number;
- (4) Purpose of examination or search;
- (5) Person(s) examining or searching records;
- (6) Person responsible for safekeeping of records, if the records are withdrawn for further examination or search; and
- (7) Name, signature, and title of person(s) requesting approval to examine or search identified records.

d. At Boulder, the Engineering, Maintenance and Support Services Division should be contacted for reference service to records in the Denver Federal Records Center, NIST-Gaithersburg, or the National Archives. Service is arranged from the Denver Federal Records Center, 24 hours or less if personal pickup is desired; from NIST Records Holding Area, 24 hours; and from the Federal Records Centers and National Archives, generally at least seven working days depending upon the exactness of the request and the channels to be followed.

2. Responsibility for Borrowed Records - No material may be removed or permanently withdrawn from a borrowed record or box of records without the knowledge and authority of

Records Management, (at Boulder, the Engineering, Maintenance and Support Services Division). **Records must be returned to storage within 30 days, unless Records Management (at Boulder, the Engineering, Maintenance and Support Services Division) is notified by memorandum.**

APPENDIX C

DISPOSITION OF NIST TEST FOLDERS AND TEST REPORTS

1. The schedule for the disposition of test folders is provided on the front of each test folder. The responsible testing official indicates the recommended retention period. The imprint is illustrated below:

DISPOSITION RECOMMENDATION	
Check the Appropriate Category for This Folder (see back cover for criteria)	
<input type="checkbox"/>	Destroy 3 years after date of certificate or report
<input type="checkbox"/>	Destroy 20 years after date of certificate or report
Signature	_____
Date	_____

2. Folders for tests of a routine nature will normally be designated for disposal after three years. Only a very small percentage of test folders will be designated for more than the three-year retention.

3. Duplicate copies of test reports maintained by the organizational units for reference purposes may be disposed of at the discretion of the chief of the organizational unit.

4. Test folders having the characteristics described below should be retained for 20 years:

- a. Those that relate to the development of new and significant testing techniques;
- b. Those that relate to new and significant arts and materials; and
- c. Those that relate to basic national and international weights and measures.

5. The National Archives may select for permanent retention additional folders if the test becomes the subject of Congressional investigation or comes under intensive public scrutiny, or if the test is involved in court decisions or legislative actions affecting the functions and activities of NIST.

6. Questions should be directed to Records Management, Management and Organization Division (at Boulder, the Engineering, Maintenance and Support Services Division).

APPENDIX D

DISPOSITION OF PAPERS COVERED BY THE PRIVACY ACT OF 1974

The Privacy Act of 1974 requires that papers subject to the Act be destroyed with adequate safeguards when they are scheduled for disposal. Records Management, Management and Organization Division, is responsible for the destruction of Privacy Act material. Privacy Act papers are destroyed as follows:

1. Privacy Act Material that is eligible for disposal can be packed in boxes (nothing larger than 18" x 11") with the lids taped shut. Archive boxes provided by Records Management should not be used for disposal material. Complete form DN-12, Disposal of Privacy Act Papers and list a brief description of material to be destroyed, including closing dates.
2. Contact Records Management (at Boulder, the Engineering, Maintenance and Support Services Division) by submitting form DN-12.
3. After receiving completed form DN-12, Records Management (at Boulder, the Engineering, Maintenance and Support Services Division) evaluates the listing of Privacy Act papers to determine if their disposal is authorized by the NIST Records Schedules and/or the General Records Schedules. If authorized for disposal at this time, Records Management arranges for pick-up of Privacy Act papers. If unauthorized for disposal at this time, Records Management notifies the contact person of the appropriate disposal date.

APPENDIX E

DISPOSITION OF RECORDS BY DEPARTING EMPLOYEES

This appendix gives guidelines for the removal or destruction of records by departing employees.

1. Guidelines for Removal or Disposition of Records

a. **Records may not be removed or destroyed by a departing employee.**

b. Personal papers may be removed or destroyed by departing employees. However, when matters requiring the transaction of official business are contained in private personal correspondence, those official business portions are to be extracted and made a part of the official files.

c. Information or documents subject to national security classification under Executive Order 12065, as amended, whether records or extra copies, shall not be removed by a departing employee. Disposition of such materials is governed by specific Department rules.

d. Information contained in documents, whether records or extra copies, which is afforded confidential or protected government treatment under various statutes or implementing rules, is not to be removed by departing employees. This information may be protected under such statutes as the Census Laws, the Export Administration Act, or 18 U.S.C. 1905 prohibiting unauthorized disclosure of confidential information relating to the business or financial affairs of identifiable business concerns. It also may be information about individuals protected under the Privacy Act of 1974 which requires the consent of such individuals, or information not made available under one or more of the exemptions contained in the Freedom of Information Act.

Questions about whether or not information in official materials is or is not subject to such government protection are to be discussed with the Counsel for NIST since these decisions are to be made only by authorized officials.

e. Departing employees may not remove any documentary information relating to any pending or contemplated civil, criminal, or administrative proceeding or other program activity when the information, if used or released on the outside, would impair or prejudice the outcome of the proceeding or government policy determinations, decisions, or other action.

2. Separation Clearance Procedure (References: Subchapter 2.06.08 and Subchapter 10.13)

Gaithersburg: Departing employees are to provide a certification on Form NIST-598, Separation Clearance Certificate, with respect to nonrecord materials which they plan to remove from NIST. The certification lists the nine Freedom of Information Act exemptions under which a government agency may decide not to make its records publicly available. These nine categories are made applicable to the nonrecord materials discussed in this appendix. For instance, general

exemption (or category) 1 applies to security classified information; exemption 3 covers materials afforded confidential treatment by various statutes; exemption 4 covers confidential business information; exemption 5 applies to interagency or intra-agency memorandums or letters which would not be available by law to party other than an agency in litigation with the agency; exemption 6 refers to personal privacy information about other persons; and exemption 7 relates to law enforcement materials. Information relating to pending or contemplated agency actions should be considered separately and treated similarly.

Boulder: Departing employees are to provide a certification on Form CD-126, Separation Clearance Certificate.

U.S. GOVERNMENT MOTOR VEHICLE OPERATOR IDENTIFICATION

Sections

2.08.01 Purpose

2.08.02 Scope

2.08.03 Definitions

2.08.04 Responsibilities

2.08.05 Operator's Identification Card (Regular Operators Only)

2.08.06 Operator Standards

2.08.07 Designation of Examiners

2.08.08 Denial or Withdrawal of Operator's Identification Card

2.08.09 Alcohol Related Convictions

2.08.10 Separations

Appendix A - Obtaining Operator's Identification Card (Regular Operators Only)

Appendix B - Traffic Records - Table of Critical Incidents

Appendix C - Positive Credit System for Regular Operators

2.08.01

PURPOSE

This subchapter gives the regulations and procedures for authorizing employees to operate government motor vehicles for official purposes. Included are procedures for the issuance and renewal of the Optional Form (OF)-346, U.S. Government Motor Vehicle Operator's Identification Card (Regular Operators), and procedures for the authorization of Incidental Operators.

2.08.02

SCOPE

The provisions of this subchapter apply to the operation of any government motor vehicle when used for official business by a NIST employee/nonemployee within the United States and its

possessions. The subchapter does not apply to employees driving privately owned vehicles on official business or to vehicles rented in the employee's name.

2.08.03

DEFINITIONS

a. Motor Vehicle - Any self-propelled mechanically or electrically powered vehicle designed to be operated principally on the highway for the transportation of property or passengers.

b. Government Motor Vehicle - A motor vehicle owned or leased in the name of the U.S. Government. The terms "NIST motor vehicle" or "assigned vehicle" used herein refers to a government motor vehicle.

c. Operator's Identification Card - OF-346, U.S. Government Motor Vehicle Operator's Identification Card.

d. Regular Operator - An employee whose position requires the operation of a government motor vehicle on a regular basis. This includes chauffeurs, firefighters, guards, and other employees with a job title of motor vehicle operator or truck driver. Employees having secondary titles of "motor vehicle operator" [i.e., gardener (motor vehicle operator)] whose principal job is not driving are considered "Incidental Operators."

e. Incidental Operator - An employee or nonemployee (Guest Researcher, Research Associate, Contractor, IPA who is working on cooperative projects with NIST and who have an occasional need to operate government vehicles), other than a regular operator, who is required to infrequently operate a government motor vehicle to carry out their official duties.

f. Road Test - The NIST standard road test, required for Regular Operators, is conducted by the Safety Office prior to the individual being assigned as a "Regular Operator." The initial road test vehicle is normally a sedan, after which the authorization to operate other vehicles (i.e. bus, ambulance, fire truck, or vehicle transporting hazardous materials) will be determined by the supervisor of the individual's operating unit.

g. State License - A driver's license issued by the state, District of Columbia, territory, or possession in which the employee is domiciled or principally employed.

2.08.04

RESPONSIBILITIES

a. The Leader, Safety Office is responsible for:

(1) Administering the government motor vehicle operator identification program and establishing supervision over the issuance of Operators' Identification Card for "Regular Operators." The NIST Safety Office has the authority to deny, restrict, or withdraw a regular operator's OF-346, or suspend an "Incidental Operator's" eligibility to operate government vehicles, based upon criteria contained in Appendix B and their judgement with regard to an employee's ability and willingness to operate vehicles safely and in compliance with rules and regulations pertaining to such operation;

(2) Informing regular operators, through their supervisors, when it is determined by the semiannual traffic record check and accident review that their eligibility status is in jeopardy with further traffic violations/accidents;

(3) Providing appropriate information for motor vehicle accident prevention training for operators of government motor vehicles, consistent with DoC requirements.

b. Supervisors of organizational units that are permanently assigned government motor vehicles, operated by regular operators are responsible for:

(1) Ascertaining that persons who operate such vehicles are authorized to do so and are in compliance with all pertinent requirements; and

(2) Promptly reporting any motor vehicle accident involving one of their employees on official business in accordance with the accident reporting requirements outlined in Subchapter 12.02.

c. Supervisors of organizational units that are permanently assigned government motor vehicles, operated by incidental operators shall:

(1) Designate those persons who are to be incidental operators of government motor vehicles assigned to their organizational units, and have those persons complete Form NIST-1283, Registration/Certification of Authorized Incidental Operators of U.S. Government Motor Vehicles Assigned to Organizational Unit; and submit to the Safety Office, annually;

(2) Ensure that only those persons who have completed Form NIST-1283 operate the assigned vehicle(s); and

(3) Promptly report any motor vehicle accident involving their assigned vehicles(s), or any of their employees/nonemployees while operating any government vehicle on official business in accordance with the accident reporting requirements outlined in Subchapter 12.02.

NOTE: The above requirements *do not* apply to organizational units that are not permanently assigned government motor vehicles.

d. Incidental Operators of government vehicles are responsible for:

(1) Having in their immediate possession a valid state driver's license for the class of vehicle they intend to operate and sign Form NIST-1283 certifying that:

(a) They have no physical/mental incapacities that are likely to affect their safe driving;

(b) Their State Driver's License has neither been suspended within the past 12 months nor revoked within the past 24 months;

(c) They have had no more than one at-fault motor vehicle accident within the past 12 months; and

(d) They have had no more than one serious (i.e., 2 or more-point assessment) moving traffic violation within the past 12 months.

(2) Maintaining cognizance of and complying with all pertinent requirements regarding the operation of government motor vehicles;

(3) Checking their assigned vehicle for safe operating condition;

(4) Reporting to the dispatcher any defect noted on the assigned vehicle;

(5) Ensuring that they and their passengers have installed safety belts properly fastened at all times when the government motor vehicle they are operating is in motion;

(6) Ensuring that cargo being transported is properly restrained to prevent movement during transit and that approved Department of Transportation placards are properly displayed when hazardous material is being transported (transport of placarded hazardous materials requires a state Commercial Driver's License);

(7) Ensuring that assigned vehicles are operated at all times in accordance with applicable traffic regulations (Parking tickets or moving violation tickets received due to the negligence of the employee while operating a government motor vehicle will be processed on their own time and at their own expense.); and

(8) Preparing the required accident reports at the scene of any accident involving the assigned vehicle and otherwise complying with the accident reporting requirements outlined in Subchapter 12.02.

Individuals who intend to requisition vehicles from the NIST Transportation Group must process Form NIST-97, Motor Vehicle Trip Request and Authorization, which can be obtained from the Transportation Group.

2.08.05

OPERATOR'S IDENTIFICATION CARD (Regular Operators Only)

a. Operating a government motor vehicle is a privilege, not a right based on one's possession of a state driver's license. An Operator's Identification Card is not a license to drive motor vehicles but rather is an authorization to operate government motor vehicles, granted on the basis of the issuing official's judgement that the holder has the ability and willingness to safely operate the types/classes of vehicles listed thereon and in compliance with rules/regulations pertaining to such operation. The Operator's Identification Card is void unless accompanied by a valid state driver's license for the class of vehicle to be operated; this fact is stamped on the reverse of each Operator's Identification Card. (NOTE: Traffic violation records on file at the various state departments of motor vehicles will be obtained and reviewed semiannually for all regular operators as herein defined).

b. No employee shall operate a government motor vehicle unless they have in their possession a valid state driver's license for the class of vehicle to be operated and a valid Operator's

Identification Card issued by NIST which specifies each type/class of vehicle they are authorized to operate and any other restrictions (eyeglasses/contact lenses, daylight driving only, on NIST grounds only, etc.) imposed upon them.

c. Employees of other federal agencies of the executive branch who operate NIST motor vehicles must comply with 2.08.04d. above.

d. The issuance of Operator's Identification Cards is restricted to Regular Operators who are required to operate government motor vehicles as a part of their official duties.

e. Operator's Identification Cards, issued to Regular Operators, are effective for not more than three years from the date of issuance and may be renewed for additional three-year periods.

f. The Operator's Identification Card must be surrendered to the issuing official on demand, when the employee's state license has been suspended/revoked or has expired or when the employee leaves NIST or moves to a position in which the driving of government motor vehicles is no longer necessary.

2.08.06

OPERATOR STANDARDS

a. Regular Operators - Office of Personnel Management rules and regulations applicable to employees classified as chauffeurs or similar full-time operators of government motor vehicles are contained in the Federal Personnel Manual Chapter 930, Subchapter 1, and are made a part of this subchapter by reference. Additionally, regular operators must meet the incidental operator minimum standards prescribed below.

b. Incidental Operators - The minimum standards for incidental operators are:

(1) Possession of a valid state driver's license for the type/class of vehicle the employee will operate; and have no violations/accidents or physical/mental incapacities that will prevent the individual from certifying/signing the statement on Form NIST-97 or NIST-1283. Individuals who have their state driver's license suspended/revoked are automatically ineligible to operate government motor vehicles. The individual shall notify their supervisor of this action, and the supervisor shall notify the Safety Office of the individual's ineligibility status.

(2) Ability to speak, read, and write the English language sufficiently to complete required reports and understand the meaning of traffic rules, regulations, control devices, etc.

2.08.07

DESIGNATION OF EXAMINERS

The Leader, Safety Office, reviews and approves the agency road test route and criteria for the grading of applicants, and assigns an adequate number of personnel to administer road tests.

2.08.08

DENIAL OR WITHDRAWAL OF OPERATOR'S IDENTIFICATION CARD (Regular Operators Only)

a. The following items constitute sufficient cause for declaring a Regular Operator ineligible to retain their OF-346 resulting in denial/withdrawal of an Operator's Identification Card and adverse action (dismissal, suspension without pay, reassignment with possible reduction in grade, etc.) as deemed appropriate:

(1) The employee's driving record (including privately owned as well as government vehicles) indicates that they are a poor risk because of unsafe driving habits or repeated traffic law violations (see Appendix B);

(2) The employee operates a government motor vehicle while under the influence of narcotics, alcohol, or other drugs/medicines that tend to impair capacity to drive safely;

(3) The employee leaves the scene of an accident involving a government motor vehicle assigned to them without making themselves known or otherwise fails to comply with accident reporting requirements;

(4) The employee is found on medical examination to fail to meet, either permanently or temporarily, the appropriate physical standards (including emotional disturbance);

(5) The employee's state driver's license is revoked, suspended, or expired;

(6) The employee is involved in a motor vehicle accident while operating a government motor vehicle and, after investigation, is found to have been grossly negligent;

(7) The employee violates traffic laws and regulations (other than those relating to parking) with a government motor vehicle;

(8) The employee improperly operates a government motor vehicle (e.g., abuse of or failure to properly maintain the vehicle); and

(9) The employee fails to comply with federal requirements related to the operation of a government motor vehicle.

b. As described in Appendix C, regular operators may accumulate positive credits which may be used to retain their eligibility by offsetting minor traffic convictions.

c. Any adverse action against a Regular or Incidental Operator shall be effected in accordance with applicable laws and regulations (see DAO 202-752), but nothing herein shall be deemed to establish any additional requirements with respect to adverse actions beyond those established by other applicable laws and regulations.

d. An individual against whom an adverse action has been taken, or whose Operator's Identification Card has been withdrawn, shall not be authorized to operate a government motor vehicle again until they demonstrate to the satisfaction of the official responsible for issuing the Operator's Identification Card that:

(1) They have reestablished their driving competence by a road test (at the discretion of the issuing official), physical examination, required course of safety instruction, or other procedures satisfactory to the official; and

(2) There is a reasonable basis to conclude that they are likely thenceforth to drive safely and in accordance with all applicable requirements.

2.08.09

ALCOHOL RELATED CONVICTIONS

a. Regular/Incidental Operators having convictions on their official traffic records for Driving While Intoxicated (DWI) or Operating Under the Influence (OUI) are not automatically considered eligible for issuance or reissuance of an Operator's Identification Card or granted eligibility one year after conviction or loss of license. For an employee/non-employee with a DWI or OUI conviction to have an Operator's Identification Card issued/reissued, or eligibility restored, it is required that the division chief of the individual do the following:

(1) For Regular Operators, sign Form NIST-1277, Application for Operator's Identification Card, as the "requesting official"; and

(2) Attach to Form NIST-1277 a memorandum to the Leader, Safety Office outlining that they have personally talked to the applicant about the DWI/OUI conviction, has conveyed management's concern for the seriousness of such violations, has warned the applicant of the consequences of subsequent convictions (i.e., loss of eligibility to operate government vehicles and potential loss of job), has made the judgement that the incident in question is not indicative of a behavioral trend but rather was an isolated incident, and recommend issuance or reissuance of the Operator's Identification Card or to otherwise restore the individual's eligibility. Note: For Incidental Operators, provide a memo to the Safety Office as prescribed in (2) above.

b. Nothing in this section shall be deemed to require reauthorization, which is discretionary with the issuing official.

2.08.10

SEPARATIONS

Employees separating from NIST are required to surrender their Operator's Identification Card during the separation clearance process.

APPENDIX A

OBTAINING OPERATOR'S IDENTIFICATION CARD

(REGULAR OPERATORS ONLY)

1. Issuance of Operator's Identification Card

a. A supervisor, having determined the necessity for an employee to operate government motor vehicles, obtains from the Safety Office the appropriate application forms for an Operator's Identification Card and processes the forms in accordance with written instructions accompanying the forms.

b. The applicant takes the following steps:

(1) Completes appropriate forms in accordance with accompanying instructions;

(2) Completes a physical examination (usually consisting of visual acuity and hearing tests only) in the appropriate Health Unit; and

(3) Completes an appropriate road test administered by a road test examiner qualified in accordance with Section 2.08.07 of this subchapter. Road test requirements are as follows:

(a) A road test, in accordance with 2.08.03f., is required for the initial issuance of an OF-346 for all Regular Operators.

(b) Supervisors of individuals who need an Operator's Identification Card should allow three work days to process the required forms and complete the required examinations.

(c) In cases involving competitive appointments to full-time driver (Regular Operator) positions, personnel actions to bring selected applicants on board are to be held in abeyance pending a determination by the Safety Office that the selected applicant is eligible for issuance of an Operator's Identification Card. For regular operator positions, satisfactory past driving performance must be determined by review of traffic records obtained from the state in which the applicant is licensed to operate motor vehicles. (It is the applicant's responsibility to provide a copy of their current official state traffic record with their application for employment in a regular operator position.) A minimum of one week should be allowed from the time the Safety Office is requested to make such determination.

(d) Upon satisfactory completion of requirements, the Safety Office issues the employee an Operator's Identification Card, indicating the type of government motor vehicles authorized to operate and any restrictions that may be applicable.

2. Renewal or Reissuance of Operator's Identification Card

- a. Approximately 45 days prior to the expiration of an employee's Operator's Identification Card, the Safety Office forwards to the employee's last known supervisor a notice of the approaching expiration and appropriate application forms for renewal. The road test is not required for renewals except in cases where the employee's driving record indicates the need to reevaluate ability to drive safely and skillfully.
- b. When the employee's Operator's Identification Card has been expired for more than 12 months, issuance of a new Operator's Identification Card is accomplished by following the procedures outlined in 1. above.

APPENDIX B

TRAFFIC RECORDS

TABLE OF CRITICAL INCIDENTS*

The following table lists traffic violations, accidents, and other serious incidents, in relation to time intervals, as examples of traffic record elements that result in denial/withdrawal of the OF-346, U.S. Government Motor Vehicle Operator's Identification Card (Regular Operator), or suspend eligibility to operate government vehicles (Incidental Operator).

INCIDENT	FREQUENCY
1. Reckless Driving	1 or more in most recent year 3 or more in most recent 5 years
2. Driving while intoxicated, under the influence of alcohol, or under the influence of a drug, a combination of alcohol and a drug, or a controlled dangerous substance.**	1 or more in most recent year 3 or more in most recent 5 years
3. Other Moving Traffic Violations	2 or more in most recent year Average of 1/year in most recent 5 years
4. State Permit Suspension***	1 or more in most recent year 3 or more in most recent 5 years
5. State Permit Revocation***	1 or more in most recent 2 years 3 or more in most recent 5 years
6. At Fault or Preventable Accidents resulting in personal injury (other than first aid) or property damage exceeding \$250.	2 in any consecutive 12-month period will result in 1 year of ineligibility from the date of second accident; Average of 1/year in most recent 5 years
7. Combinations of above incidents (i.e., moving violations and accidents) will also result in	

denial/withdrawal of the individual's OF-346, or suspension of the individual's authorization to operate government vehicles.	
---	--

*This list represents limits that are automatically disqualifying unless the Operator's Identification Card applicant/holder (Regular Operator only) has positive credits (described in Appendix C) to offset an applicable minor incident. The Safety Officer has the additional responsibility to judge each case individually and to deny or withdraw the Operator's Identification Card/suspend eligibility of any individual whose record indicates an inability or unwillingness to safely operate a motor vehicle or an unwillingness to comply with rules/regulations pertaining to such operation. The decision to deny or withdraw an Operator's Identification Card/suspend eligibility may be based upon a severe individual incident or violation pattern. The Safety Officer also has the authority and obligation to limit or restrict authorized operators to on-site driving or to specific classes of vehicles based on past driving record or other indications that such limitations are in the best interest of the government.

**See Section 2.08.09 for special provisions regarding DWI or OUI convictions.

***Section 2.08.05b. and 2.08.06b.(1) reflects federal policy that an Operator's Identification Card/authorization to operate government vehicles is automatically invalid unless the operator has in their possession a valid state driver's license for the class of vehicle being operated. Regular or Incidental Operators who have their state driver's license suspended/revoked must not operate a government motor vehicle, notify their supervisor of the action, and (if applicable) immediately return their Operator's Identification Card to the Safety Office. (NOTE: Persons who have their state driver's license suspended/revoked and who are subsequently issued a restricted state driver's license for employment and educational purposes will still lose eligibility to operate government motor vehicles under the criteria in Items 4 and 5, above). If a Regular or Incidental Operator has their state driver's license suspended/revoked at any time, promptly notifies their supervisor, and (if applicable) returns the Operator's Identification Card to the Safety Office as required, the eligibility will be invalid for one full year from the date of suspension of the state license and for two full years from the date of revocation of the state license. Otherwise, the one-year (suspension) or two-year (revocation) period of ineligibility to operate government motor vehicles will start on the date that the Safety Office becomes aware of the holder's state license suspension/revocation. Failure to promptly notify their supervisor and (if applicable) return Operator's Identification Cards to the Safety Office could also result in additional adverse actions.

APPENDIX C

POSITIVE CREDIT SYSTEM FOR REGULAR OPERATORS

The Positive Credit System is intended to provide "limited" consideration for Regular Operators based on their established good driving record. Under this system a driver may earn one credit for each three years of violation/accident-free record based on the government experience and state traffic record. Regular Operators currently holding a valid OF-346, U.S. Government Motor Vehicle Operator's Identification Card, will have their driving records reviewed back to January 1, 1986, for the purpose of establishing positive credits. A new applicant for an Operator's Identification Card will have their driving record reviewed back three years from the date of application for the purpose of establishing credit [maximum of one credit for new applicants].

Violations/accidents that may be offset by these credits are:

1. Moving violations not resulting in accidents such as:

a. Speeding, less than 10 MPH above the posted speed limit

b. Stop/Yield sign violations

c. Lane change violations

d. Other types of minor moving violations for which conviction results in no more than a one-point assessment.

2. Accidents:

Property damage resulting in not greater than \$1,000 repair costs for vehicle(s) and/or property involved.

Violations/accidents for which credits may not be used:

1. Speeding 10 MPH or more above the posted speed limit

2. Reckless driving

3. Other moving violation convictions which result in more than a one-point assessment.

4. Driving under the influence of intoxicants or narcotics

5. State suspensions/revocations

6. Incidents involving multiple violations/citations.

7. Failure to wear seat belts

8. Accidents resulting in personal injury (beyond first aid) or losses greater than \$1,000 for repair of vehicle(s) and/or property.

In the event a regular operator who has accumulated one or more positive credits through their established good driving record is involved in an incident as described above, for which a positive credit may be used, they would use one of these credits to avoid being placed in a situation that would result in ineligibility should another incident occur, as described in Appendix B. The credit totals for each regular operator are maintained by the Safety Office through the semiannual traffic record check of the state driving record. A regular operator may only use one positive credit during any twelve-month period to offset an applicable traffic violation or property damage accident.

AUDITORIUMS AND CONFERENCE ROOMS

Sections

- 2.12.01 Purpose
- 2.12.02 Scope
- 2.12.03 Legal Authority
- 2.12.04 Policy
- 2.12.05 Delegations of Authority
- 2.12.06 Responsibilities
- 2.12.07 Auditorium and Conference Room Uses
- 2.12.08 Audiovisual Technical Services
- 2.12.09 Equipment for Loan
- 2.12.10 Dining Rooms A, B, and C
- 2.12.11 Exhibits, Displays, and Training Aids
- 2.12.12 Recording Presentations and Discussions
- 2.12.13 Content Owner
- 2.12.14 Effective Date

Appendix A – Guidelines and Policies for Scheduling and Use of Auditoriums and Shared-Use Conference Rooms

Appendix B – Auditoriums and Shared-Use Conference Rooms-(Gaithersburg Campus)

Appendix C- Standard AV Equipment and Services in Auditoriums and Shared-Use Conference Rooms-(Gaithersburg Campus)

Appendix D- Audio Video Recording Release

Appendix E- Auditorium and Shared-Use Conference Rooms (Boulder Campus)

2.12.01

PURPOSE

This subchapter states NIST policy and procedures for using auditoriums and NIST-wide shared-use conference rooms.

2.12.02

SCOPE

The provisions of this subchapter apply to NIST-Gaithersburg and NIST-Boulder.

2.12.03

LEGAL AUTHORITY

15 U.S.C. 271 et seq.

2.12.04

POLICY

a. The primary purpose of Institute auditoriums and conference rooms is to provide a place where scientific and technical groups may meet to conduct official business and for NIST-wide meetings and events. These rooms may also be used for internal training and meetings that cannot be conducted in OU and/or divisional conference rooms.

b. Auditoriums and conference rooms are available only upon assignment, subject to the conditions prescribed in this subchapter.

2.12.05

DELEGATION OF AUTHORITY

The NIST Director has delegated supervision of auditoriums and conference rooms (listed in Appendix A) to the Audio-Video Services Group under the Public and Business Affairs Office. (At NIST/Boulder Laboratories, supervision of auditoriums and conference rooms has been delegated to the Office of the Director, NIST/Boulder Laboratories.)

2.12.06

RESPONSIBILITIES

a. Meetings held in Institute auditoriums and conference rooms must be attended by at least one NIST employee. This person, acting as the sponsor or meeting coordinator, assumes responsibility for the proper use of NIST facilities and equipment and ensures the following:

(1) All meetings and events with more than 35 external participants must be coordinated with the Conference Program Group, Public and Business Affairs Office (see NIST Administrative Manual Subchapter 14.06), and Form NIST 1176 and/or Form NIST 1176A are submitted for these meetings. When required, a DN 16 form is also submitted along with proof of insurance coverage (see paragraph 2.12.07.b (5)(ii))

(2) All visitors have appropriate badges as required by the Emergency Services Division (Gaithersburg campus).

(3) Furniture is left in the same configuration in which the room was found.

(4) Equipment dedicated to the room is not removed and any loaned equipment is returned to Audio-Video Services Group.

(5) All conference materials and trash are disposed of in room receptacles and/or removed.

(6) All laptops, USB drives, CDs and DVDs used for meetings are removed, and any documents and files used on room-based computers are deleted. If presenters have logged onto room computers, they have logged off.

(7) Any technical problems are reported to the Audio-Video Services Group.

b. The Audio-Video Services Group schedules conference rooms (at Boulder, the Office of the Director, NIST/Boulder Laboratories). The Audio-Video Services Group (at Boulder, the Office of the Director, NIST/Boulder Laboratories) is authorized to change room assignments if in its judgment it is in the interest of the Institute to do so.

c. The Audio-Video Services Group (at Boulder, the Engineering, Maintenance and Support Services Division (EMSS)) provides audiovisual (AV) services and is responsible for the set up, operation of and removal of and/or shutting down of equipment. In some cases, users will be given training in the use of audiovisual equipment, and in these cases the users are responsible for the use and operation of that equipment.

d. The Conference Program Group, Public and Business Affairs Office (at Boulder, the Conference Program Group):

(1) Provides general assistance in advance planning of conferences and symposia;

(2) Ensures that the promotion activities preceding meetings and the actual meetings are run smoothly and professionally; and

(3) Provides the participants with services required at such meetings.

2.12.07

AUDITORIUM AND CONFERENCE ROOM USES

a. Assignments are made for the following uses:

(1) Institute-sponsored meetings to carry out the assigned functions of the Institute (at NIST/Boulder Laboratories, DoC-sponsored meetings):

(i) Internal – NIST (DoC) staff only; [in NIST/Boulder Laboratories, NIST, NTIS and NOAA (DOC)]

(ii) Advisory or other panel groups which include professionals who are closely associated with NIST (DoC); and

(iii) General conferences or symposia, including associated Institute activities attended by non-NIST employees from professional groups or societies.

(2) Federally sponsored training programs;

(3) Meetings or sponsored activities of the Standards Employees Benefit Association (SEBA) and the Boulder Laboratory Employees Association (BLEA); and

(4) Subject to the Institute's needs, NIST auditoriums and conference rooms may be made available as follows:

(i) Professional and government organizations whose purposes are clearly related to the work of the Institute (Department);

(ii) Charitable, civic or other organizations who have requested and been granted special permission from the Office of the Director

b. Permission to use auditorium and conference rooms is subject to the following conditions:

(1) Meetings and activities should be held in a manner that is appropriate for a federal agency. For example, meetings may not be held primarily for commercial, political or religious purposes or for the purpose of advocating or influencing action on legislation. Questions regarding appropriateness should be directed to the Director, Public and Business Affairs.

(2) Reservations may be cancelled in unusual circumstances where space must be reallocated for NIST (or DOC) mission critical reasons. (at NIST/Boulder Laboratories, DoC). Every effort will be made to allocate alternative space should this be necessary.

(3) Meeting rooms are not available for assignment to any organization, individual, or activity practicing or advocating discrimination based on race, color, religion, gender, national origin, age, physical or mental disabilities or sexual orientation.

(4) Nongovernmental organizations and groups are not permitted to use meeting rooms as a regular meeting place.

(5) Insurance for nongovernment users:

(i) Any nongovernment organization authorized to use a NIST auditorium, conference room, or other facility must, prior to approval for such use, submit for review an insurance policy which:

-- satisfactorily protects and holds harmless the United States of America, the Department of Commerce, and the National Institute of Standards and Technology, its officers, agents, servants, and employees from liability for any and all claims made under the Federal Tort Claims Act, as amended (28 U.S.C. 2671-2680) for damage to property, or as the result of injury or death to any person occurring in connection with the use of the Institute's premises; and

-- by endorsement or otherwise, lists NIST as a coinsured.

(ii) Prior to approval of the use of the Institute's premises, groups must fill out and submit Form DN 16 and in so doing agree in writing to pay for damage to or destruction of any Institute property occurring in connection with the use of the Institute's premises and must furnish written evidence of their financial responsibility to fulfill this obligation.

(iii) The insurance company used by the nongovernment organization or group must be one which is authorized to do business in the states of Maryland, for use of the NIST Gaithersburg facility, or Colorado, for use of the NIST/Boulder Laboratories, by the governmental agencies controlling insurance companies in the states of Maryland or Colorado.

(iv) The insurance policy submitted pursuant to the requirements of this paragraph must be forwarded through the Conference Program Group (at NIST/Boulder Laboratories, the Office of the Director, NIST/Boulder Laboratories), to the Chief Counsel for NIST for review and determination as to acceptability before approval of the use of the Institute's premises may be granted.

(6) Users of the auditoriums (at NIST/Boulder Laboratories, the Auditorium and Room 1107) are not permitted to operate the projectors or control booth equipment. When such services are required, arrangements must be made with the Audio-Video Services Group for AV Technicians to operate the equipment.

(7) No admission fee may be charged for the use of meeting rooms. However, registration fees may be collected to cover expenses incurred in holding a conference. (see NIST Administrative Manual Subchapter 14.06).

(8) NIST may require reimbursement for services provided to a conference. All fee-supported conferences are charged a conference management fee by the Conference Program Group. In addition, reimbursement may be required for AV technicians, NIST police, furniture movers, janitorial services and/or for services and equipment not normally available through the Audio-Video Services Group (such as webcasting, webinars, satellite broadcasting, etc.).

(9) The serving or consumption of food or beverages in auditoriums is prohibited. Serving or consumption of food or beverages is only allowed in lecture rooms with prior permission from the Audio-Video Services Group. Requests should be made directly to the Manager, Audio Video Services Group.

(10) No electrical apparatus, special equipment, or mounted decorations may be used, and no changes in fixtures and furnishings may be made, unless approved by the Audio-Video Services Group (at NIST/Boulder Laboratories, the Office of the Director).

(11) Auxiliary AV equipment may not be connected into existing systems without explicit permission from the Audio-Video Services Group (at NIST/Boulder Laboratories, the Office of the Director).

(12) All persons attending meetings are subject to rules and regulations of the National Institute of Standards and Technology and are required to comply with instructions given by the Emergency Services Division. Conference attendees must be escorted by a NIST staff person when they are in (or passing through) restricted areas of the campus or during restricted hours (6:30 p.m. to 7:00 a.m. each workday and all day Saturdays, Sundays, and holidays).

(13) Prior to the start of each meeting, the meeting sponsor must ensure that participants are informed of proper exiting procedures for cases of emergency evacuation. For meetings held in the auditoriums, a slide (or other image) must be shown that visually references these exits. (An appropriate slide is available from the Audio-Video Services Group for incorporation directly into presentations.)

(14) Meetings and Conferences with over 35 external attendees must coordinate program planning with the Conference Program Group, PBA. (See NIST Administrative Manual Subchapter 14.06, paragraph.01)

(15) An interpreter for the deaf and other appropriate accommodations (such as wheelchair lift, assistive listening device, etc.) are made available for all NIST-wide internal meetings. For meetings where external attendees will be present, advance materials should state that all requests for accommodations be directed to the program sponsor and if requested these accommodations should be made available. The meeting sponsor is responsible for ensuring that these accommodations are available.

2.12.08

AUDIOVISUAL TECHNICAL SERVICES

a. At NIST Gaithersburg, the Audio-Video Services Group provides AV technicians in both auditoriums to operate and monitor the equipment and in other lecture rooms for video recording and other services as required (at Boulder, the Engineering, Maintenance and Support Services Division provides these services).

b. Audiovisual equipment is categorized in two ways: equipment that must be operated by an AV technician and equipment that may be used and operated by the user.

(1) In general, lecture rooms are set up with equipment that is easily operated by the user (such as data projectors, microphones, etc.). To use or be trained in this equipment, users should contact the Audio-Video Services Group.

(2) Auditorium equipment located in the projection booths and equipment located in Building 101, Room B-114 (Control Room in Gaithersburg (At NIST/Boulder Laboratories, Building One Auditorium and Room 1107) may only be operated by AV Services technicians.

2.12.09

EQUIPMENT FOR LOAN

a. The Audio-Video Services Group (in Boulder- the Engineering, Maintenance and Support Services Division) has a variety of projection, video and audio recording and audio amplification equipment available for loan for use at official Institute functions. If requested, the Audio-Video Services Group will provide instruction on the use of equipment.

b. In cases where the equipment is lost or stolen, the borrowing organizational unit provides from its depreciable equipment or other appropriate cost center the funds necessary to purchase a replacement. If the borrowing organizational unit is without equipment money during the fiscal year in which the loss is incurred, the borrowing organizational unit must allocate equipment money from the next fiscal year for replacement.

2.12.10

DINING ROOMS A, B, AND C (Gaithersburg)

a. Dining Rooms A, B, and C are intended primarily for luncheon conferences. These rooms are to be used from 11 a.m. to 2 p.m. for non- luncheon conferences only when other rooms are not available.

b. Dining Rooms are scheduled through the Audio-Video Services Group, and food arrangements are made as follows:

(1) Self- Service Luncheons. Participants purchase lunch from the cafeteria and then remove all trays and place on cafeteria-supplied tray carts located in Dining Room hallway

(2) Served luncheons are arranged through the Conference Program Group, Public and Business Affairs Office.

2.12.11

COMMERCIAL EXHIBITS AND DISPLAYS

The use of commercial exhibits and displays in any of the auditoriums, conference rooms, or adjacent corridors must be cleared in advance with the Manager, Audio-Video Services Group (At NIST/Boulder Laboratories, clearance by the Office of the Director, through the Conference Program Group is required). Use must comply with the following limitations:

a. Products and exhibits are respectful and fair on issues of gender, national origin, disability, religion, age, race, color and sexual orientation.

b. The sale of merchandise, solicitation of orders, or materials designed to solicit business for a particular company product, rather than an industry, is prohibited in NIST conference rooms unless given specific permission by the Chief Facilities Management Officer.

c. Vendor exhibits or equipment demonstrations that are being held in conjunction with a specific conference should be coordinated with the Conference Program Group.

d. Safety and fire regulations must be strictly observed. See NIST Administrative Manual Subchapter 6.07 Building 101 Corridor Utilization Policy.

e. The National Institute of Standards and Technology is not responsible for loss or damage to exhibits.

f. Exhibits must be erected without damage to the building and must be physically self-supporting.

g. The exhibitor is responsible for moving the material into the building, setting it up, and dismantling it upon completion of the exhibit. The exhibitor must arrange in advance with the Audio-Video Services Group for any necessary storage of boxes and supplies during the exhibit period. Only very limited storage exists for exhibits, and storage space may not be available at all. All cartons, crates, etc. must be removed from the building promptly after the closing date.

h. Exhibits should be moved into buildings through loading platforms and only through building lobby entrances when given explicit permission from the NIST Police. (in NIST/Boulder Laboratories, by the Office of the Director through the Conference Program Group)

i. Permission for the use of amplified sound as part of an exhibit must be requested in advance from the Audio-Video Services Group (in NIST/Boulder Laboratories, the EMSS Division) and when permitted, must be conducted at a moderate volume.

j. Equipment demonstrations for the NIST staff by a particular company must be approved in advance by the Chief, Acquisition Management Division. Approval or disapproval depends upon the nature of the

demonstration. The Institute employee requesting the approval makes all arrangements for appropriate space, etc. for the demonstration.

k. Equipment demonstrations for the NIST staff by an industry or a single company must, prior to approval of the use of the Institute's premises, agree in writing (through the submittal of form DN 16) to pay for damage to or destruction of any Institute property occurring in connection with the use of the Institute's premises, and must furnish written evidence of their financial responsibility to fulfill this obligation.

2.12.12

RECORDING PRESENTATIONS AND DISCUSSIONS

a. Before any recording is made of the participants at conferences or meetings, the speakers must be advised and consent to this recording. The responsibility for complying with this requirement rests with the meeting's sponsor or program chairperson.

b. The Audio-Video Services Group (in NIST/Boulder Laboratories, the Conference Program Group) will not proceed with any recording (audio or video) of non-federal government presenters unless their signed permission has been documented on the approved consent form ("Audiovisual Recording Release" available through the Audio-Video Services Group, see Appendix D) and a copy of all signed ("Audiovisual Recording Release") forms are given to the Audio-Video Services Group.

c. Recorded presentations are maintained by and available from the organizational unit sponsoring the program.

2.12.13

CONTENT OWNER

107- Public and Business Affairs

2.12.14

EFFECTIVE DATE October 1, 2009

APPENDIX A

Guidelines and Policies for Scheduling and Use of Auditoriums and Shared-Use Conference Rooms

1. Institute employees planning a meeting should contact the Audio-Video Services Group for room reservations and AV support (at NIST/Boulder Laboratories, contact the Office of the Director).
2. Organizers of meetings and conferences of 35 or more external attendees must coordinate directly with the Conference Program Group (in Gaithersburg or Boulder) before scheduling rooms.
3. Organizers of meetings with external attendees must submit a NIST-1176 and/or NIST 1176A form (and DN 16-when appropriate for insurance liability) to the Conference Program Group prior to the date of the meeting.
4. If food service is desired, the sponsor should contact the Conference Program Group for arrangements for served luncheons, VIP receptions and coffee breaks for conferences, and symposia. Appropriated funds may not be expended on food or beverages; such items may only be purchased for conferences through the No-Cost Contractor, which is overseen by the Conference Program Group.
5. Requests from state and local governments and outside organizations should be made in writing to the Director, Public and Business Affairs Office (at NIST/Boulder Laboratories, to the Office of Director through the Conference Program Group). The insurance policies required in Section 2.12.08.5 for nongovernment users must accompany this written communication. The written communication (in the form of a letter or email) should include the following information:
 - name of the person responsible for the meeting;
 - purpose of the meeting;
 - general description of the audience to whom the meeting is addressed;
 - room(s) desired;
 - date and time (beginning and ending) of meeting;
 - approximate number of people attending;
 - what AV support is required and
 - other special equipment or arrangements necessary.
6. In cases where final meeting dates have not been chosen and multiple dates are requested, rooms will be put on “hold status” rather than “reserved status”. If another requester is interested in the room, then the original requester will have three days to confirm their requirement. In general, requesters will not be allowed to hold more than two dates for meetings where dates have not been finalized.
7. Full-day meetings with primarily external audiences will be given priority in the Green Auditorium. Partial day, internal meetings of 100 or less will be scheduled in the Portrait Room, the Red Auditorium or other suitable room. Two weeks prior to the event date, requesters may ask to switch to the Green Auditorium if preferred. If it is available, the event will be rescheduled for that room. (In NIST/Boulder Laboratories, full-day meetings will be given priority in the Building One lobby rooms, including the auditorium, 1103, 1105 and 1107)
8. Lecture rooms will be set in a “standard configuration” (see Appendix B for listing). All efforts should be made to use the room in that setup. Requests for non-standard seating arrangements may require overtime or other charges and should be requested with at least three days advance notice. Last minute requests may not be fulfilled.
9. The Portrait Room, the Heritage Room and the Advanced Measurement Laboratory main conference room (C103/C106) will only be reset by the Plant Division’s movers (rather than the Audio-Video Services Group)

and costs charged to the division accordingly if other than standard configuration is requested. Customers must submit work orders directly to the Plant Division with a copy to AV Services.

10. Rooms will only be reset by the Audio-Video Services Group and/or the Plant Division (in NIST/Boulder Laboratories the EMSS Division) for full-day or multi-day meetings. (In NIST/Boulder Laboratories, organizers of meetings that require multiple resets will be required to submit a work order to the EMSS Division and may incur additional charges).

11. Rooms may only be reserved for the actual time of the meeting plus reasonable time to set up and take down materials, etc. Rooms may not be booked for the entire day for the purpose of avoiding other policies such as: #8, #9 or #10.

12. In rare cases, customers will be given permission to reconfigure furniture themselves (e.g. for partial day meetings). This requires explicit permission from the Audio-Video Services Group (in NIST/Boulder Laboratories, the Office of the Director). If customers are given permission to reset a room, they will be responsible for resetting it back to its standard configuration before the next scheduled meeting begins.

13. Lecture Rooms A, B and D will be considered comparable and interchangeable. If moving a previously scheduled meeting from one room to the other will allow a multi-day meeting or conference with external attendees to take place, the original meeting will be relocated. If an event is relocated for this purpose, the Audio-Video Services Group will ensure that the room to which the meeting is moved is configured as originally requested.

14. Organizers of multi-day training and events that require multiple lecture rooms--essentially taking over the entire conference area -- must first request permission from the Manager, Audio-Video Services Group (in NIST/Boulder Laboratories, the Office of the Director through the Conference Program Group).

15. Meetings may not be reserved more than one year in advance. Some exceptions will be made (e.g. for scientific conferences that require multiple years of advance notice and ongoing NIST required meetings). Permission for these exceptions will be granted by the Manager, Audio-Video Services Group.

16. Conferences and business meetings will always take precedence over social events and unofficial, non-business activities. These events may be bumped from rooms for business-related activities and will be given as much notice as possible.

17. Audiovisual technicians are available through the Audio-Video Services Group between the hours of 7 am and 5:30 pm ET (in NIST/Boulder Laboratories through the EMSS Division between 7:30 am and 5 pm MT). Services requested outside of these hours may require staff to work overtime, and organizers will be charged accordingly. These charges will be billed through the Audio-Video Services Group (in NIST/Boulder Laboratories, the Conference Program Group or the EMSS Division).

APPENDIX B

Auditoriums and Shared-Use Conference Rooms (Gaithersburg Campus)

Room Name	Room Style	Standard Configuration	Capacity
Green	Auditorium *	Theater Style	294
Red	Auditorium *	Theater Style	722
LR A	Lecture Room	Theater Style	80
LR B	Lecture Room	Theater Style	80
LR C	Lecture Room	Classroom Style	30
LR D	Lecture Room	Classroom Style	60
LR E	Lecture Room	Classroom Style	48
LR F	Conference Room *	U-shape Style	20
B-111	Conference Room *	Conference Style	15
B-113	Conference Room *	Conference Style	15
Portrait Room	Lecture Room #	Theater Style	120
Heritage Room	Multi-Purpose Room #	Cluster Style	63
Cafeteria-West Wing	Dining Area *	Dining Area	48
DR A	Conference Room *	Conference Style	12
DR B (Director's DR)	Conference Room +	Conference Style	12 (combined w/DRA=24)
DR C	Conference Room *	Conference Style	24
AML C103/106	Lecture Room #	Classroom Style	80

- * Rooms with permanent configurations that cannot be reset.
- + To reserve DR B, permission must first be granted by the Director's Office. This room may also be combined with DR A, if arrangements have been made with the Audio-Video Services Group.
- # Rooms that are reset by Plant Division's movers, not by the Audio-Video Services Group.

Appendix C- Standard AV Equipment and Services in Lecture Rooms (Gaithersburg)

The following list can be used as a general guideline for equipment available in each room, but users should speak directly with the Audio-Video Services Group staff when planning to use the AV equipment. To ensure that AV equipment is set up properly, it must be requested in advance with the Audio-Video Services Group.

Room	Standard Equipment (see note a)	Standard AV Services (see note b)
Green Auditorium	Fully equipped with AV support (incl. PC @ podium).	Data and video projection, video and audio recording, video and conferencing and other services as requested.
Red Auditorium	Fully equipped with AV support (incl. PC @ podium).	Data and video projection, video and audio recording, video and conferencing and other services as requested.
Lecture Room A	Data/video projector, audio amplification, screen, podium, VTC- if requested.	Data and video projection, video and audio recording, video and conferencing and other services as requested.
Lecture Room B	Data/video projector, audio amplification, screen, podium, VTC- if requested.	Data and video projection, video and audio recording, video and conferencing and other services as requested.
Lecture Room C	Data/video projector, audio amplification, screen, podium, VTC- if requested.	Data and video projection, video and audio recording, video and conferencing and other services as requested.
Lecture Room D	Data/video projector, audio amplification, screen, podium, VTC- if requested.	Data and video projection, video and audio recording, video and conferencing and other services as requested.
Lecture Room E	Data/video projector, audio amplification, screen, podium	Data and video projection, video and audio recording and other services as requested
Conference Room F	2- 50" plasma flat screens, VTC if requested, DVD playback	Data and video displayed through plasma screens, video and audio conferencing and other services as requested
Conference Room B-111	Data/video projector, screen, VTC – if requested	Data and video projection, video and audio conferencing and other services as requested.
Conference Room B-113	Data/video projector, screen, VTC – if requested	Data and video projection, video and audio conferencing and other services as requested.
Portrait Room	Fully equipped with AV support (incl. PC @ podium)	Data and video projection, video and audio recording, video and

		audio conferencing and other services as requested
Heritage Room	Data/video projector, audio amplification, screen, podium,	Data and video projection, audio amplification, podium and screen
Cafeteria –West Wing	No AV equipment as standard	Data and video projection and if requested.
Dining Room A	No AV equipment as standard	Data and video projection and if requested.
Dining Room B (Director’s DR)	No AV equipment as standard	Data and video projection and if requested.
Dining Room C	Data/video projector, screen	Data and video projection
AML C103-C106	Fully equipped with AV support (incl. PC @ podium)	Data and video projection, video and audio recording.

Notes

- a. Listed AV equipment is standard, however any equipment that users plan to utilize should be requested when room is scheduled or minimally three days in advance.
- b. AV services are available as listed in rooms; however, any service that users plan to utilize should be requested when a room is scheduled. Standard services such as video/data projection, VTC with Boulder, audio conference phones should be scheduled at least three days in advance. Specialized AV services such as video and audio recording, webcasting, video teleconferencing (with non-Boulder sites) and interconnecting with other web services (webinars, etc.) must be scheduled at least two weeks in advance to ensure that technical needs can be met.
- c. Wireless internet is available in all auditoriums and conference rooms. NIST laptops must be configured to receive wireless (contact iTAC for instructions). Visitors should contact their NIST sponsor for instructions on connecting their laptops.

Appendix D:

U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY			
AUDIOVISUAL RECORDING RELEASE			
REQUESTER	ORGANIZATION CODE	TELEPHONE EXTENSION	DATE
FULL NAME OF THE MEETING		STOCK TAPE OR MEDIA PROVIDED YES NO	ADDITIONAL SERVICE REQUIRED YES (PLEASE FILL SERVICE REQUEST LOG)
LOCATION OF THE MEETING	RECORDING FORMAT	COMMENTS	
<p>By signing this form, I irrevocably grant to the National Institute of Standards and Technology (NIST), U.S. Department of Commerce, or any person acting under the direction of NIST the right to record my likeness on any audiovisual format including film (still photo and/or motion picture) and/or videotape, or in any other medium to copyright said digital format, film and/or videotape, to edit, crop and duplicate such recording at NIST's discretion, to record my voice on digital hard-disc, magnetic tape, to incorporate the same photographic and/or video images and audio recordings into digital or analog audio-video program and to use or authorize the distribution and use of the program and any subsequently edited or altered versions thereof in any manner and media at any time or times throughout the world in perpetuity, and to use my name, likeness, recorded voice or biographical information in connection therewith, including promotion in all media.</p> <p>I hereby release NIST and anyone authorized by NIST to use said photographic and/or video images, audio recordings or other materials concerning me from any and all claims, damages, liabilities, costs and expenses which I now have or may hereafter have by reason of any use thereof.</p> <p>I understand that all media, video, audio, or other materials produced by the NIST, U.S. Department of Commerce, will be the property of NIST and subsequently in the public domain.</p>			
SPEAKER (print name)		SPEAKER release signature	DATE
RECORDED BY TECHNICIAN (S)	DATE (S)	COMMENTS	
<p>As chair/organizer of a meeting refereed above, I _____ have obtained the above permission for all participant presenters listed below. Their written consent is attached if not signed below.</p>			
Name	Signature	Date	

Appendix E

Auditoriums and Shared-Use Conference Rooms (NIST/Boulder Laboratories Campus)

APPENDIX E Boulder Conference Rooms

			Room Set		Equipment Available															
Building	Conference Room	Capacity	Default	Classroom Style	Black Board	Audio Conferencing	Data (LCD) Projector	Flip Chart	Internet Connection	Microphone System	PA System	PC Hookup	PC Training	Projection Screen	Speaker Phone	Telephone Connections	TV/VCR	Video Conferencing	Video Recording	White Board
1	1103	30	Theatre	15 @ Tables		X	X	X	X	X	X	X		X		X	X			X
1	1105	30	Theatre	15 @ Tables		X	X	X	X	X	X	X		X	X	X	X			X
1	1103/1105	60	Theatre	30 @Tables		X	X	X	X	X	X	X		X		X	X			X
1	1107	75	Theatre	40 @ Tables		X	X	X	X	X	X	X		X	X	X	X	X	X	X
1	Auditorium	502	Theatre*	N/A	2	X	X		X	X	X	X		X		X	X	X	X	

1	2565A	12	8 @ Conference Table	N/A										X						X
1	4020	20	10 @ conference	16-20 @ Tables			X	X	X					X	X	X	X			X
1	4511 (Boulder II)	12	12 @ Conference Table*	N/A			X							X				X		
1	4550 (Boulder 1)	12	12 @ Conference Table*	N/A		X Ext 7497	X							X			X	X		
1	4552	24	Theatre	18 @ Tables		X	X	X						X	X		X			X
1	4560A	12	12 @ Computer Stations*	N/A			X						X	X						
1	5000 (Boulder III)	12	12 @ Conference Table*	N/A		X Ext 5503	X							X	X			X		X
2	0113	58	Theatre	28 @ Tables			X	X						X			X	X		X

* Rooms with permanent configurations that cannot be
reset

PROCEDURES FOR APPROVAL OF NIST MEMBERSHIPS AND STAFF PARTICIPATION IN PROFESSIONAL ORGANIZATIONS

3.02.09 Procedures for Approval of NIST Memberships and Staff Participation in Professional Organizations

A. NIST Institutional Membership in a Professional Organization -

- 1) Memberships and technical committee participation in professional organizations are allowed with supervisory approval as long as the membership does not entail voting, or service on boards or other policy-making committees.
- 2) All approved NIST institutional memberships for professional organizations are noted on the List of Professional Organizations maintained by the Management and Organization Office. It is NIST's policy that NIST may not become a member of an organization that is not listed on this Institutional Membership roster.
- 3) With respect to professional organizations, requests for approval of a NIST institutional membership not on the list should be sent to the NIST Chief of Staff with a clearance section signed off by the Office of the Chief Counsel for NIST. The Office of the Chief Counsel for NIST will review the organizational documentation to determine whether NIST institutional membership is legally permissible. Individual NIST employee memberships in professional organizations may not be accepted or funded by NIST. The request should include a memo cleared by the division and signed by the OU Director or designated management, addressed to the NIST Chief of Staff. The charter and bylaws of the organization and a link to their website should be attached to this memo. The Chief of Staff forwards all findings to the requestor for noting and to the Management and Organizations Office for listing.

B. Service on Boards or Other Policy-making Bodies and Government Liaisons -

- 1) Invitations to serve on a board or other policy-making body of a professional organization require legal review by the Ethics Division of the DoC Office of General Counsel. After approval by the Ethics Division, a staff member who is invited to serve on a board or other policy-making body of a professional organization must forward a memo detailing the proposed service and its benefits to NIST, through their management chain and the Chief Counsel for NIST, to the Director, Standards Coordination Office, for approval. This request for NIST approval should include a recommendation as to the voting or non-voting status of the proposed participation.
- 2) Government Liaisons - Alternatively, NIST representatives can serve in the role of government liaison to an organization when NIST needs to exchange nonproprietary information or coordinate activities. A liaison's role is limited to matters in which NIST has an interest, not internal matters unrelated to NIST's interests. The role is limited to providing technical guidance or any other activity that furthers the

agency's mission as determined by NIST program officials. Note also that service as a government liaison is conditioned upon approval by NIST management and the organization's agreement to this arrangement. Please also note that government liaisons may not receive compensation and may not serve as the organization's agent or representative.

C. Fees for Professional Organizations -

- 1) Fees for Professional Organization Institutional Membership - Institutional membership fees for professional (non-standards) organizations may be paid only to professional organizations currently on the approved list maintained by the Standards Services Group. NIST organizational units may elect to pay for institutional membership fees for approved professional organizations by using direct (i.e., STRS) or indirect appropriated funds (transferred from other agencies for this purpose) or funds generated by overhead.
- 2) Professional Organization Individual Memberships - Except as may occur pursuant to NIST Administrative Manual Subchapter Section 10.08.10(1), NIST has no authority for payment of professional (non-standards) organization individual memberships.

TELECOMMUNICATIONS SERVICES

4.04.01 - CONTENTS

- 4.04.02 Purpose
- 4.04.03 Scope
- 4.04.04 Legal Authority
- 4.04.05 Policy
- 4.04.06 Delegation of Authority
- 4.04.07 Responsibilities
- 4.04.08 Procedures
- 4.04.09 Content Owner
- 4.04.10 Effective Date

4.04.02 - PURPOSE

This subchapter states policies and procedures for using and obtaining telecommunications services for official business.

4.04.03 - SCOPE

This subchapter applies to all NIST Gaithersburg & Boulder Federal employees and Associates.

4.04.04 - LEGAL AUTHORITY

- a. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401),
- b. Office of Management and Budget (OMB) Circular A-130,
- c. National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook).
- d. Department of Commerce Administrative Order 201-39.
- e. Department of Commerce Telecommunications Management Policy.

4.04.05 - POLICY

Use of Telecommunication Services – Federal government telecommunication services (including facsimile, calling cards, mobile and other wireless devices and services) are intended for the conduct of official business. Employees are authorized to utilize these services for limited personal use, provided that such use does not interfere with official business, create appreciable costs to NIST or embarrass NIST or the Department of Commerce. Questions about uses for which appropriateness is not clear to a staff member should be directed to local management.

Prohibitions - The following practices are specifically prohibited:

- a. Use of Federal government telecommunications services for other than official business, except in cases of acceptable limited personal use described above.
- b. Personal use of any Federal government-provided telecommunications service, equipment, or facility that significantly interferes with the conduct of Government business or the individual performance of the employee.
- c. Unauthorized telecommunications use with the intent to later reimburse the Federal government.
- d. Use of Federal government telecommunications services for partisan political purposes or activities.
- e. Use of toll-based or similar calling services that places a toll burden on the Federal Government, such as 900 area code services.

Collect and Third Party Telephone Calls - Collect calls (calls placed from a non-Federal government number to a Federal government number, reversing charges) and third party calls (calls placed through an operator and billed to a telephone number other than either the calling or called telephone numbers) are prohibited except for official business. A personal emergency call may be accepted without authorization, but should be reported to a supervisor. In mission locations and offices where a "call-in" capability is required, the use of Federal government-provided toll-free services (such as 800 area code) should be considered.

Toll Free Numbers for NIST Employees - While conducting official government business offsite, employees can contact NIST (Gaithersburg) toll-free via 1.800.437.4385. This number is for NIST employees only and should not be given to or used by other individuals for use in calling NIST. Boulder's toll free number to access phonemail only is 1.800.579.5383.

Calling Cards - Federal government-issued calling cards should only be used for placing telephone calls when on official government travel or telecommuting. A calling card is for use only by the employee to whom it has been issued; calling cards or card numbers should not be given to or used by other individuals.

Reimbursement for Privately Owned Telecom Services - The Federal government may not require employees to acquire or use their own personally owned services for the purpose of performing their official duties. However, under certain circumstances, Federal government employees may be reimbursed for the use of their own, privately owned telecommunications services when acceptable Federal government-owned service is not available and reimbursement is in the best interest of the Federal government.

The amount of reimbursement must be the actual cost of service as shown on the employee's billing statement. Reimbursement may not cover the basic cost of service already owned by the employee, only the incremental, additional cost for use of the service for Federal government-related work. Employees may not be reimbursed for use of personally owned or acquired services for which they have not incurred any incremental additional costs due to such use (for example, the use of a personal mobile phone for official calls, when the individual's phone usage for the entire month remains below the monthly free minute quota). If an employee uses more than the allocated or permitted number of "free" calls or minutes under a vendor's billing plan, the employee may be reimbursed at the additional call or minute rate multiplied by the number of calls or minutes used

for Federal government business, but such reimbursement shall not exceed incremental additional costs incurred by such use. In all such cases, reimbursement must be approved by the employee's management, either before or after use.

Federal Government Provided Resources in Private Residences - With prior approval of management and when done in accordance with Federal Acquisition Regulations, NIST may use appropriated funds to install telecommunications lines, equipment, or services and to pay monthly charges in any private residence of an employee who has been authorized to work at home. Refer to NIST Administrative Manual, Subchapter 10.27 for further guidance on the Telework Program. Lines, equipment or services paid for by the Federal government are subject to the same limitations to official use as outlined above.

Monitoring of Telephone Conversations - Monitoring of telephone conversations for law enforcement purposes is covered by DoC security policies and DAO 207-9. For purposes other than law enforcement, monitoring of telephone conversations may be performed in certain circumstances with strict limitations, as outlined in the DoC Telecommunications Management Policy. Prior to establishing a system that will record or monitor conversations or transmissions, a request must be made to the Department of Commerce.

Tampering with Federal Government Owned Equipment or Facilities - NIST staff shall not install, disconnect, rearrange, remove, or attempt to repair any equipment or facilities. Costs incurred due to unauthorized tampering that requires a service repair call will be billed to the staff member's organization.

4.04.06 - DELEGATION OF AUTHORITY

The NIST Director has delegated to the Chief Information Officer (CIO) the authority to approve NIST Telecommunications policy.

4.04.07 - RESPONSIBILITIES

Each NIST staff member (both Federal employees and Associates) having access to an official Federal government telephone is responsible for its proper use.

Supervisors are responsible for proper management of Telecommunications services and costs, and for taking appropriate disciplinary action against employees and others under their jurisdiction that abuse the service.

Approving officials are responsible for proper management of mobile devices and must review the invoices and take appropriate actions to ensure that the policies are followed.

The respective Telecommunication Offices (Gaithersburg and Boulder) are responsible for the approval of all requests for telecommunications service so that the resources can be effectively managed. The Telecommunication Offices are also responsible for compliance with current regulations, the procurement of cost-effective telecommunications services, and for the maintenance of complete, current, accurate billing records, and the inventory of services in use.

The Gaithersburg Telecommunications Office is the contact for information exchange with the Office of Radio Frequency Management, Department of Commerce, for the purpose of application for frequency assignment, radio frequency management reports, and resolution of harmful interference to or from NIST radio operations. The Gaithersburg Telecommunications Office is responsible for providing policy guidance and technical and administrative support to all staff and organizational units within NIST (Gaithersburg & Boulder). NIST frequency management activities operate under the guidance of National Telecommunications and Information Administration (NTIA). Reference: National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency (Redbook) and the Department of Commerce Administrative Order 201-39.

4.04.08 - PROCEDURES

Request for Telecommunication Services - Applications for telecommunications services (obtain, move, add, change, or terminate) must be submitted to the Telecommunications Office.

Request for Radio Frequency Assignment – Applications for radio frequency assignments at Gaithersburg or Boulder may be submitted by sending an e-mail to telecom@nist.gov. The request should include the proposed use, geographic area of proposed use, and approximate power requirement.

Repair Request - For telephone repair service, dial x5375 (iTAC) in Gaithersburg and Boulder. Additionally Boulder staff can submit a repair request located on the Boulder Telecom website.

General Information – For general information regarding NIST telephone and telecommunications services and to access the service/repair request forms staff members should contact OCIO.

4.04.09 - CONTENT OWNER

The OCIO Telecommunications and CIO Support Division are responsible for the content of this policy.

Guidance on this policy may be obtained from the OCIO's:

Telecommunications Office
Mail Stop 1851
301.975.3333
telecom@nist.gov

4.04.10 - EFFECTIVE DATE

February 1, 2010

CORRESPONDENCE

Sections

4.05.01 Purpose

4.05.02 Scope

4.05.03 Policy

4.05.04 Definitions

4.05.05 Responsibilities

4.05.06 Mail Referred by DOC

4.05.07 Correspondence with Officials at DOC

4.05.08 Clearance of Correspondence

4.05.09 Answering Public Inquiries

4.05.10 Answering Complaints

Appendix A - Preparation of Correspondence at NIST

Appendix B - Examples of Guidelines Contained in Appendix A

Appendix C - Assembling a Letter for Signature

Appendix D - Example of NIST Control Ticket

Appendix E - Example of Preferred Format for a Memorandum Prepared at NIST

Appendix F - International Correspondence

4.05.01

PURPOSE

a. This subchapter outlines NIST procedures and responsibilities for correspondence handling, preparation, and signing. It is also a supplement to the Department of Commerce Executive Secretariat Manual which is available by accessing <http://home.osec.doc.gov/ExeSec/default.htm>.

b. Special rules for handling classified correspondence are covered in Subchapter 13.01.

c. Special rules for handling Congressional correspondence are covered in Subchapter 4.06.

4.05.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

4.05.03

POLICY

a. All correspondence is to be prepared promptly and in the manner that is most helpful to the recipient and at the least cost to the government.

b. Formal communications must be on official stationery and must be prepared in accordance with government correspondence standards for appearance and style as covered in this subchapter.

c. The Director must be kept aware of all correspondence that is politically sensitive or has policy implications. (Read Section 4.05.04d.) The original of such correspondence must be cleared by the Chief Counsel for NIST, Congressional and Legislative Affairs, and the Chief of Staff before mailing. An information copy of all such letters, with a copy of the incoming correspondence, must be furnished to the Director.

4.05.04

DEFINITIONS

a. Correspondence - All mail, faxes, e-mail, cables, telexes, and other media of record.

b. Memorandum - An internal means of communication. Appendix E gives a formatted example of a memorandum as used at NIST.

c. Official File Copy - A hardcopy format (paper) record of all formal government communications. This copy must be placed in the organizational unit's files. It is the copy that will be retired by NIST Forms and Records Management. A copy needed for personal files should be prepared as an information copy.

The requirement for an "official file" copy is based on a government-wide regulation that records be maintained to document the transaction of public business "as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data."

d. Policy correspondence - Deals with program direction and with legislative and legal questions as follows:

(1) Discussions of proposals for new Institute programs and modifications of existing programs;

(2) Correspondence on politically sensitive matters;

(3) Correspondence on legal matters;

(4) Correspondence on proposed or pending program, authorization, or appropriation legislation with:

- members of Congress
- Congressional committees
- Congressional staff
- officials at the White House
- officials at all government agencies
- influential members of the public.

Correspondence on any subject with members or staff of Congressional committees or subcommittees which act on NIST authorization or appropriations or are otherwise of special importance to NIST is always treated as policy correspondence and must be cleared through the NIST Director of Congressional and Legislative Affairs, the Counsel for NIST, the Program Office, and the Budget Division.

e. Priority mail is to be answered within a specified time. Priority mail includes mail referred to NIST by the DOC, the White House, or the Congress for the preparation of a response to be signed by an official at NIST, the DOC, or the White House. Priority mail is correspondence determined to be of sufficient importance to require a timely response and is controlled so that it can be tracked and monitored. (Read Sections 4.05.06 and 4.05.07.)

4.05.05

RESPONSIBILITIES

- a. The Office of the Director is responsible for correspondence policy at NIST. Correspondence practices at NIST are followed within the guidelines established by the DOC.
- b. The OU office is responsible for all controlled correspondence assigned to their OU including the quality and timeliness of the response.
- c. NIST staff must be aware of and be responsible for communications concerning their assigned program responsibilities and follow the formats and guidelines in this subchapter and the DOC Executive Secretariat Manual.
- d. Writers are responsible for the technical and policy content of the letters they draft, clear, or sign, for answering correspondence promptly, and for adhering to the guidelines in this subchapter.
- e. Mail and Distribution (at Boulder, the MASC Mail Room) is responsible for the receipt, routing, collection, and dispatch of most mail and for ensuring that postal regulations are followed.
- f. The Director, NIST/Boulder Laboratories, is responsible for determining whether any correspondence reviewed by that office requires clearance and/or the signature level.

g. The Office of International and Academic Affairs is responsible for coordination and clearance of official communications with foreign countries. (Read Appendix F.)

h. The Communications and Inquiries Group (at Boulder, Publications) is responsible for answering or referring public inquiries.

i. The Office of the Director is responsible for maintaining a follow-up system on controlled mail and referring such correspondence and other mail addressed to the Director to the appropriate individual or organizational unit for reply.

The Office of the Director also ensures proper coordination and clearance of replies, dispatches correspondence signed by the Director and Deputy Director, and distributes copies of this correspondence.

4.05.06

MAIL REFERRED BY DOC

The DOC Executive Secretariat Manual (<http://home.osec.doc.gov/ExeSec/default.htm>) contains instructions on handling mail forwarded directly from the White House and instructions on complying with Executive Secretariat control tickets.

4.05.07

CORRESPONDENCE WITH OFFICIALS AT DOC

a. The Information Memorandum, Decision Memorandum, and Signature Memorandum are used to correspond with the Secretary and Deputy Secretary. Contact the Office of the Director for the current format and requirements for these memoranda.

b. A memorandum is used to correspond with other officials at the Department. (Read Appendix E.)

4.05.08

CLEARANCE OF CORRESPONDENCE

When correspondence is sent to an official for clearance, that official initials and dates if they concur. If the official does not concur, then the appropriate organizational units take action to resolve any issues.

4.05.09

ANSWERING PUBLIC INQUIRIES

a. Inquiries from the public addressed to "NIST" are referred by Mail and Distribution to the Communications and Inquiries Group (at Boulder, Publications) for reply. These organizational units may ask for assistance from the technical staff or refer the inquiry to a technical organizational unit for preparation of a reply.

b. Inquiries from the public addressed to an individual or an activity are answered by the appropriate organizational unit unless they deal with a politically sensitive issue. Inquiries not directed to the proper organizational unit should be referred to the

Communications and Inquiries Group (at Boulder, Publications) for reply or for referral to the proper organizational unit or individual.

c. A courteous and informative reply to a public inquiry should be prepared and dispatched promptly. If an answer will be delayed beyond a few days, the inquiry should be acknowledged and the date given when a reply can be expected.

4.05.10

ANSWERING COMPLAINTS

Complaints about NIST services are forwarded to an official at least one level higher than the organizational unit about which the complaint is made (division chief or higher). The division chief or higher prepares, clears, or signs the reply to ensure that it is responsive. A reproduced copy of the complaint and an information copy of the response are sent to the Office of the Director through the OU office.

USE OF DESIGNATED NIST FACILITIES FOR PROPRIETARY AND NON-PROPRIETARY MEASUREMENTS

Sections

5.01.01 Purpose

5.01.02 Scope

5.01.03 Policy

5.01.04 Legal Authorities

5.01.05 Use and Approvals

5.01.06 User Charges

5.01.07 Roles and Responsibilities

5.01.08 Conditions for Use

5.01.09 Handling Measurement Results Under a Proprietary Measurement Agreement

5.01.10 Handling Measurement Results Under a Non-Proprietary Measurement Agreement

Appendix A - Determination of Fees for Proprietary and Non-Proprietary Measurements

5.01.01

PURPOSE

This subchapter states the policies and procedures to be followed in using designated NIST facilities for independent proprietary, collaborative proprietary, and non-proprietary measurements, including conditions under which such use is allowed, approval is given, and fees are established and collected. The purpose is to support government policy for enhancing U.S. international competitiveness by providing U.S. industry access to special U.S. government facilities to advance technology and strengthen productivity.

5.01.02

SCOPE

The policies and procedures outlined in this subchapter apply only to NIST facilities which are specifically designated by the NIST Director.

5.01.03

POLICY

Under certain conditions, NIST allows the independent use of specific measurement and test facilities by private parties for proprietary, collaborative proprietary, or non-proprietary use. A User Agreement is required for each of these uses; they differ in the treatment of any resulting intellectual property and technical data.

5.01.04

LEGAL AUTHORITIES

20 U.S.C.91

15U.S.C. 3710a

DAO 202-311, Section 5.02. a2

DAO 202-311, Section 5.02. b1 DoC Accounting Principles and Standards Handbook, Chapter 11, Section 4.0, available online at

<http://www.osec.doc.gov/ofm/acctg/Chapter.11%20revised%2008-2007.doc>

OMB Cir. A-25, available online at <http://www.whitehouse.gov/omb/circulars/a025/a025.html>

5.01.05

USE AND APPROVALS

a. Agreements are used for independent research where such use is infrequent, temporary, and irregular.

b. Agreements may be for as long as five years or the duration of the security assurance/clearance, whichever is shortest, provided that the users endeavor to conclude their use of the facility as expeditiously as possible.

c. Collaborative Proprietary Agreements are used when the research is relevant to the mission of NIST and where the results of the research must be kept confidential and withheld from disclosure for a period of up to five (5) years and where NIST research expertise are necessary to the success of the research project.

d. The following approvals are required:

(1) Independent proprietary or non-proprietary agreements

OU Director or the Facility Manager (if authorized for this purpose by the OU Director) signs the Agreement on behalf of NIST;

(2) collaborative proprietary agreements - OU Director or the Facility Manager (if authorized for this purpose by the OU Director) signs the Agreement on behalf of NIST; - Chief of the Office of Technology Partnerships; - NIST Counsel; and - Budget Division (for user charges).

5.01.06

USER CHARGES

a. User charges are required for proprietary use of NIST facilities and are determined by the facility as authorized by the OU Director. User charges for non-proprietary use are optional, but if charges are made for one party, they must be made for all parties in accordance with an equitable system pre-approved by the OU Director and the NIST Counsel; OU Directors may identify facilities under their supervision that will not impose user charges for non-collaborative, non-proprietary work.

b. Following regular procedures and to offset expenses, the OU establishes an Expense and Income Project and collects charges according to a schedule appropriate for such projects.

5.01.07

ROLES AND RESPONSIBILITIES

- a. The OU Director recommends to the NIST Director (via memorandum with a copy to the Industrial Partnerships Program) those facilities in their Laboratories that should be considered for proprietary or non-proprietary measurement use.
- b. The NIST Director designates facilities for proprietary and/or non-proprietary measurement use.
- c. The potential user submits a written request for use (via an approval memorandum) identifying the specific facility, type of use (proprietary or non-proprietary), duration of use, reason for use, and other pertinent information, to the NIST OU Director.
- d. The NIST OU Director or the Facility Manager, if authorized for this purpose by the OU Director, reviews and approves each request for use, ensures that the conditions specified therein for such use are met, provides equal opportunity of use through wide public notice, and ensures that the information specified below is provided to the Industrial Partnerships for collaborative proprietary agreements.
- e. In the case of collaborative proprietary use agreements, the Office of Technology Partnerships prepares the Collaborative Proprietary Facilities Use Agreement upon receipt of the approval memorandum and accompanying information from the OU Director, obtains the requisite signatures and approvals, and maintains permanent records of:
 - (1) the designation of the facility;
 - (2) individual requests for use;
 - (3) signed approval memorandum;
 - (4) the Agreements; and
 - (5) annual schedule of user charges (from Budget Office).
- f. All facilities in which information technology resources (e.g., computer equipment) are used to collect, process, or store proprietary information must be accredited as sensitive information systems prior to operation. System managers should consult with their OU Computer Security Officer or the NIST Computer Security Officer for help in the accreditation process.

5.01.08

CONDITIONS FOR USE

- a. Alternative facilities of equal or superior performance are not otherwise readily available to the user.
- b. Costs are borne by the user on a full-cost basis for proprietary use, except for specially identified user facilities.
- c. Such use does not interfere with the execution of NIST programs or present a danger of harm to NIST staff, the users, or the facilities.
- d. Such use is subject to termination at any time at the discretion of NIST.
- e. Users meet the DoC/NIST security requirements established for non-employees.

f. In providing equal access to facilities, OU Directors and facilities managers may prioritize and schedule requests for use according to the needs of ongoing NIST programs

5.01.09

HANDLING RESULTS OBTAINED UNDER A PROPRIETARY FACILITIES USE AGREEMENT

- a. To preserve the proprietary nature of the data which result from use of its facilities, the user must obtain the measurement data directly and exclusively from the apparatus.
- b. A private organization retains the entire right, title, and interest to any inventions resulting from the research performed by its employees under a Proprietary Facilities Use Agreement.

5.01.10

HANDLING RESULTS OBTAINED UNDER A COLLABORATIVE PROPRIETARY FACILITIES USE AGREEMENT

- a. The user and NIST work collaboratively to obtain data from the use of the facilities. NIST may assist the user in the conduct of the research and the collection of data.
- b. Data that results from collaborative work under a Collaborative Proprietary Facilities Use Agreement may be protected by NIST from disclosure for a period of up to five (5) years.
- c. Inventions resulting from research are owned by the inventing party. Inventions made jointly by NIST and the user are jointly owned.
- d. Non-NIST employees may not participate as part of the NIST research team in the conduct of research and the collection of data.

5.01.11

HANDLING RESULTS OBTAINED UNDER A NON-PROPRIETARY FACILITIES USE AGREEMENT

Results under a Non-Proprietary Facilities Use Agreement are non-confidential, and NIST will permit public access to available results. NIST is also entitled to use the resulting data for its own purposes. (—)

APPENDIX A

DETERMINATION OF FEES FOR PROPRIETARY AND NON-PROPRIETARY MEASUREMENTS

1. Introduction

Private organizations or individuals who are granted permission to use NIST facilities for proprietary measurements are required to reimburse NIST on a full cost recovery basis. For non-proprietary measurements, user charges are optional but must be applied equitably to all users. Non-proprietary user charges may range from no-charge to full-cost recovery. Budget Division review is not needed for non-proprietary measurement user charges. Prior to entering into an agreement, the Budget Division approves (on a fiscal year basis) the amount to be charged for each facility. The OU Director of each facility must determine what constitutes the full cost of using the facility. The OU Director should retain a permanent record of what factors were included in the calculation of "full cost." Charges should be explainable to potential users, and differences in charges to various users should be defensible in the event that user fees are audited.

The factors that should be included in the calculation of "full cost" are largely a function of the services provided. It is anticipated that generally there will be two levels of services offered.

- a. NIST Labor Intensive - A service whereby NIST staff members are actively involved in carrying out the measurement, in addition to the general administration of the agreement.
- b. Non-Labor Intensive - A service whereby only minimal NIST staff effort would be required in initially instructing people how to use the facility as well as staff time devoted to the general administration of the agreement.

2. Guidelines for Charging Costs and Setting Fees

Costs for proprietary measurements can be estimated and must be recorded in a separate expense and income project for each agreement. Alternatively, if accounting data currently exist which record the cost of operating and maintaining the facility, then that data can be used to develop an hourly or daily rate by dividing total costs, including all overheads, by the number of days or hours the facility is available for use.

The following checklist should be used in initially calculating the fees:

- a. How much NIST staff labor will be required (including technician or clerical support)?
- b. What types of special services or supplies are required which will be supplied by NIST?
- c. Are incremental costs incurred as a result of this measurement being performed?

3. NIST Labor Intensive Services

Full cost recovery can be achieved by charging for technical labor directly involved in providing a service and maintaining the facility as well as any clearly identifiable other objects expenses. Indirect management costs, general administrative costs, utility expenses, and amortization of equipment are automatically recovered through the application of overhead charges on the direct labor in the appropriate expense and income project for proprietary measurements. The Building Depreciation and DoC Overhead Surcharge is also automatically recovered on direct labor that is charged to the expense and income projects for proprietary measurements (see Subchapter 8.08, Appendix F).

In those instances, where the charges for proprietary measurements represent a repayment of costs paid with STRS, the costs associated with the proprietary measurements should be determined and then transferred from STRS to the appropriate expense and income project. When Form NIST-94 is prepared, it should include an additional amount for the Building Depreciation Surcharge. The income for the Building Depreciation Surcharge should be credited to project 5981999 in the Office of the Chief Financial Officer. All other income should be credited to the appropriate proprietary measurement project.

4. Non-Labor Intensive Services

For those agreements that require only minimal NIST staff effort, the following mechanism is suggested for calculating a full cost recovery fee. Charge the client for each person using the facility a fee equal to the average total overhead charges (Division, Laboratory, Institutional Support, and Building Depreciation Surcharge) paid per staff person per NIST technical workday or workweek in the organizational unit making the facility available. In billing the client, the Finance Division should be instructed to credit Institutional Support, Laboratory, and Division overhead accounts for the respective portions of the overall fee. Contact the OU Office and the Budget Division for the appropriate project number to be credited. The Building Depreciation Surcharge should be credited to project 5981999.

This mechanism eliminates the tedious accounting that would otherwise be involved in recording small amounts of technical, management, and clerical labor; depreciation, training, maintenance of equipment, and incidental supplies. It also provides coverage for general NIST management and operation of the NIST sites at Gaithersburg and Boulder, including utility expenses.

5. Special Requirements Imposed by the Sponsor

Occasions may arise, under either labor-intensive or non-labor intensive agreements, where special conditions or configurations are required by the sponsor. In such instances, the full cost to create such conditions and, if appropriate, to restore the facility to its original order, should be included in cost estimates.

6. Items Not Appropriate for Cost Recovery

- a. Upgrading of facilities.
- b. Recovery of initial investment.

Sections

CONTENTS

5.03.01 Purpose

5.03.02 Scope

5.03.03 Legal Authority

5.03.04 Policy

5.03.05 Delegations of Authority

5.03.06 Responsibilities

5.03.07 Enforcement

5.03.08 Examples of Advertising

5.03.09 Content Owner

5.03.10 Effective Date

5.03.01

PURPOSE

This subchapter cites regulations, delineates NIST policy, and provides guidance on compliance in typical situations regarding the use of the NIST name in advertising.

5.03.02

SCOPE

This subchapter applies to all NIST employees when there is a possibility that private sector organizations, especially businesses, may wish to use the NIST name in their product or service literature or advertising.

5.03.03

LEGAL AUTHORITY

15 CFR 200.113

5.03.04 POLICY

It is NIST policy to follow the federal regulations regarding the use of its name in advertising as outlined in Section 200.113 of Title 15 of the Code of Federal Regulations:

"As the national standards laboratory of the United States, NIST maintains and establishes the primary standards from which measurements in science and industry ultimately derive. It is therefore sometimes desirable for manufacturers or users of measurement standards to make appropriate reference to the relationship of their calibrations to NIST calibrations. The following considerations must be borne in mind, and shall be understood as constituting an agreement on the part of the NIST customer to be bound thereby in making reference to NIST calibration and test reports.

"The results of calibrations and tests performed by NIST are intended solely for the use of the organization requesting them, and apply only to a particular device or specimen at the time of its test. The results shall not be used to indicate or imply that they are applicable to other similar items. In addition, such results must not be used to indicate or imply that NIST approves, recommends, or endorses the manufacturer, the supplier, or the user of such devices or specimens, or that NIST in any way 'guarantees' the later performance of items after calibration or test.

"NIST declares it to be in the national interest that NIST maintain an impartial position with respect to any commercial product. Advertising the findings on a single instrument could be misinterpreted as an indication of performance of other instruments of identical or similar type. There will be no objection, however, to a statement that the manufacturer's primary standards have been periodically calibrated by NIST, if this is actually the case, or that the customer might arrange to have NIST calibrate the item purchased from the manufacturer.

"NIST does not approve, recommend, or endorse any product or proprietary material. No reference shall be made to NIST or to reports or results furnished by NIST in any advertising or sales promotion which would indicate or imply that NIST approves, recommends, or endorses any product or proprietary material, or which has as its purpose an intent to cause directly or indirectly the advertised product to be used or purchased because of NIST test reports or results.

"In its own activities as a scientific institution, NIST uses many different materials, products, types of equipment, and services. This use does not imply that NIST has given them a preferential position or a formal endorsement. Therefore, NIST discourages references, either in advertising or in the scientific literature, which identify it as a user of any proprietary product, material, or service. Occasionally effective communication of results by NIST to the scientific community requires that a proprietary instrument, product, or material be identified in an NIST publication. Reference in an NIST publication, report, or other document to a proprietary item does not constitute endorsement or approval of that item and such reference should not be used in any way apart from the context of the NIST publication, report, or document without the advance

express written consent of NIST."

The policy on the use of the NIST name has been expanded to include NIST-traceable reference materials and NIST-developed software/algorithms. Accordingly, NIST, in cooperation with commercial firms, may produce and characterize reference materials which are directly traceable to NIST and are, therefore, labeled "NIST traceable reference materials." Further, commercial firms may produce computer software which incorporates NIST-developed algorithms. The producer shall be allowed to cite NIST as the source of those specific portions of the product by the inclusion of the phrase, "Incorporates NIST-developed software/algorithm." These citations do not mean, and should not be implied to mean, evaluation, endorsement, or certification of commercial firms' products and services.

5.03.05

DELEGATIONS OF AUTHORITY

The Director of Public and Business Affairs, in consultation with the Chief Counsel for NIST, has authority to implement this policy.

5.03.06

RESPONSIBILITIES

It is the responsibility of the Director of Public and Business Affairs (PBA) or his/her designee, in consultation with the Chief Counsel for NIST, to answer questions from external organizations or NIST staff about this policy. It is the responsibility of all NIST staff who notice violations of this policy in advertisements or company literature to report these violations to PBA.

5.03.07

ENFORCEMENT

Violations of this policy will be enforced through written requests from Public and Business and Affairs to external organizations requesting their compliance and explaining the purpose of the NIST policy. In the event that these organizations ignore written requests from PBA, the Office of Chief Counsel for NIST will follow up with additional written correspondence and legal action if necessary.

5.03.08

EXAMPLES OF ADVERTISING

Five typical examples of advertising are given, showing activities which are prohibited and which are acceptable.

EXAMPLE 1

The XYZ Instrument Company reads a NIST technical paper in the open literature describing the design of a new type of instrument developed as part of a NIST research project. XYZ likes the design and decides to manufacture and sell an instrument based on this design, which they refer to as an "XYZ/NIST Instrument" both in their advertising and on the front panel of the instruments.

COMMENTARY: While NIST encourages commercial firms to utilize the results of NIST research to the greatest extent possible, the use of NIST's name in association with a proprietary product in that manner is prohibited! Even if the advertising copy and product literature were to make clear NIST's lack of involvement in the commercial venture, the possible implication that NIST is involved with this particular product is contrary to the policy stated above that NIST maintain an impartial position with respect to commercial products and also causes concern on the part of the manufacturers of competing instruments.

RECOMMENDATION: In this case, the manufacturer should have limited mention of NIST to stating that XYZ's design of the instrument is based on technical information published by NIST (and reference the appropriate technical paper) or *based* on a NIST design.

EXAMPLE 2

A manufacturer labels a product it manufactures as "NIST traceable" or prominently displays this phrase in its advertising.

COMMENTARY: Many Federal regulations and contracts require regulated organizations or contractees to demonstrate that the measurements that they make are "traceable" to national standards. NIST encourages this practice but at the same time cannot condone the prominent display of its name on proprietary products or in the advertising of them. This particular use of NIST's name clearly implies NIST's endorsement contrary to our policy as stated above.

RECOMMENDATION: The manufacturer in this case could have described in some detail how their product is calibrated. This could include a discussion of how their laboratory standards are related to national standards through direct calibration by NIST or indirectly through an intermediate calibration laboratory. As long as this description is factual and the NIST name is not prominently displayed, NIST would encourage such practice.

EXAMPLE 3

An organization claims by virtue of NIST calibration or test reports, that NIST "certifies" its standards.

COMMENTARY: NIST does not "certify" customer standards or products, since the word "certify" carries a connotation of a warranty or guarantee. Obviously, NIST cannot warrant or guarantee the quality or reliability of standards or products calibrated by NIST once they leave NIST following calibration. Even high quality standards do drift with time, and NIST test reports make clear that the value assigned to a calibrated standard is only valid in a rigorous sense at the time that the calibration was performed at NIST.

RECOMMENDATION: Organizations should limit the use of NIST's name to factual statements such as "Our standard cells are submitted to NIST for recalibration at intervals of approximately two years."

EXAMPLE 4

An organization produces a reference material in cooperation with NIST, samples the material, determines uniformity and characteristics, provides samples to NIST for final characterization, and then sells the remainder of the lot as NIST TRACEABLE REFERENCE MATERIALS.

COMMENTARY: These materials have been measured by the manufacturer and by NIST for uniformity and characteristics. A well documented sampling process and measurement chain exists. NIST favors the use of such materials and may authorize the use of the term NIST TRACEABLE REFERENCE MATERIALS.

RECOMMENDATION: Use of the term NIST TRACEABLE REFERENCE MATERIALS is restricted to reference materials that have been manufactured offsite, rigorously sampled, and then characterized by NIST.

The term "NIST Traceable Reference Material" is permissible only for reference materials which are (1) manufactured and characterized by a commercial company, then (2) rigorously sampled, and (3) then finally characterized by NIST using the samples from the original lot.

EXAMPLE 5

A software manufacturer labels a product as NIST-approved by virtue of incorporating NIST-developed software or algorithms in the program.

COMMENTARY: NIST encourages industry use of NIST-developed software or algorithms in commercial software and the acknowledgement by industry of such use. However, NIST should not be represented as certifying or endorsing commercial software because NIST has no control over how the software or algorithms were incorporated and used.

RECOMMENDATION: The manufacturer can cite the incorporation of NIST-developed software or algorithms without implying that NIST has evaluated, endorsed, or certified the commercial software product.

5.03.09

CONTENT OWNER

Director, Public and Business Affairs

5.03.10

EFFECTIVE DATES

June 30, 2009

Administrative Manual Section 5.04 Non-Reimbursable Technical Assistance by NIST

Sections

- 5.04.01 Purpose
- 5.04.02 Scope
- 5.04.03 Policy
- 5.04.04 Definition
- 5.04.05 Criteria
- 5.04.06 Responsibilities

5.04.01 PURPOSE

This subchapter states the guidelines for and prescribes the procedures to be followed in carrying out, recording, and reporting non-reimbursable technical assistance. For reimbursable work, see Subchapter 5.12, Contract Research Performed by NIST for Non-Federal Parties.

5.04.02 SCOPE

The provisions of this subchapter apply to all NIST employees.

5.04.03 POLICY

It is NIST policy to provide non-reimbursable technical assistance when the performance of such services in no way impedes the accomplishment of NIST objectives and when they may be of benefit to and in support of the NIST mission. NIST staff may not collect a fee for these or related services on a private basis. Such services may be undertaken only as a part of their regular duties, subject to management approval.

5.04.04 DEFINITION

Technical assistance is the provision of assistance or information in response to inquiries from another NIST organizational unit, another federal agency, a non-federal government organization, or the general public. The time spent is usually of short duration. It may include one or more written responses, a telephone call, discussions with a visitor to NIST, visits to a non-NIST site, or a combination of several of these situations. More than one individual may be involved in providing technical assistance.

5.04.05 CRITERIA

- a. NIST receives numerous requests for advice and assistance on problems relating to areas falling within the NIST mission. These requests are not continuous, predictable, or of significant magnitude to require reimbursable agreements. Before providing technical assistance on a non-reimbursable basis, each supervisor should make the following determinations:

- (1) The assistance is not of a magnitude to require cost recovery (see Section 5.04.06);
 - (2) The assistance does not impede the accomplishment of the objectives of work on funded projects; and
 - (3) The assistance provides a means of exchanging information of mutual benefit.
- b. Unless special cost centers are established, non-reimbursable technical assistance services are to be charged to a cost center most closely related to the activity.

5.04.06 RESPONSIBILITIES

a. Supervisors are responsible for being aware of any significant total and individual non-reimbursable technical assistance performed by their staff. Services are deemed significant as outlined below:

- (1) Any single request for technical assistance requiring the equivalent of eight hours.
- (2) If numerous requests are received routinely from the same source, non-reimbursable technical assistance that cumulatively total 10 percent (4 hours) of an individual staff member's time per week are deemed significant.
- (3) Numerous requests, regardless of source, for non-reimbursable technical assistance that cumulatively total 15 percent (6 hours) of an individual staff member's time per week shall be deemed significant.

b. Division chiefs have the responsibility for establishing guidelines or procedures to be followed by their staff and have final responsibility for the waiver of charges for all technical assistance provided by their staff. Depending on the extent of this activity, organizational units may initiate the following actions:

- (1) Establish an STRS technical assistance cost center against which expenses for non-reimbursable assistance services are charged;
- (2) Develop specific instructions and procedures for clearing, reporting, and keeping records of significant total and individual non-reimbursable technical assistance provided by each staff member; and
- (3) If routine records are not kept, periodically assess the magnitude of technical assistance services to obtain a reasonable estimate of these activities for the purpose of ensuring proper management of staff and other resources.

c. The NIST Director, NIST Deputy Director, or OU Director (or their designees) may from time to time require division chiefs to provide reports on the extent and nature of their technical assistance services to assess the overall OU or NIST activities. This information must be provided from existing records or appropriately conducted surveys.

PROTECTING THE CONFIDENTIALITY OF PROPRIETARY INFORMATION RECEIVED BY NIST

Sections

5.06.01 Purpose

5.06.02 Scope

5.06.03 Policy

5.06.04 Legal Authority

5.06.05 Responsibilities

5.06.06 Conditions for Use

5.06.07 Approval Procedures

5.06.01

PURPOSE

This subchapter states the policy and procedure for protecting the proprietary information received by NIST from external organizations or persons. Proprietary information includes trade secrets, commercial, and financial information submitted to NIST. Divulging or improperly using such information without the express permission of the owner is a criminal violation of the Trade Secrets Act (18 U.S.C. 1905).

5.06.02

SCOPE

a. This subchapter applies to all NIST employees.

b. The provisions of this subchapter are not applicable in instances where proprietary information is received via a proposal process (e.g., ATP, MEPP, procurement, grants, and contracts) for announced competitions for which special provisions apply.

5.06.03

POLICY

NIST encourages the exchange of scientific and technical information. However, it is also NIST policy to decline the receipt of proprietary information unless it is absolutely necessary. If the proprietary information is necessary, parties must implement a Cooperative Research and Development Agreement (CRADA) or Non-Disclosure Agreement before proprietary information can be received.

5.06.04

LEGAL AUTHORITY

18 U.S. C. 1905

5.06.05

RESPONSIBILITIES

NIST employees receiving proprietary information are responsible for knowing whether it is considered proprietary

by the provider. Consequently, NIST employees must request advance notice of the possible disclosure of an organization's proprietary information if a discussion and/or meeting is to be held with the organization. If a CRADA or Non-Disclosure Agreement has not been signed, NIST employees should be prepared to decline receipt of proprietary information (oral or written) and/or exit a meeting if the organization insists on disclosing such information.

5.06.06

CONDITIONS FOR USE

a. A Non-Disclosure Agreement should be in place prior to the receipt of proprietary information by NIST employees from an external party. A separate Non-Disclosure Agreement is not needed by NIST project team members to receive proprietary CRADA-related information from a CRADA partner. The CRADA already provides for the protection of such information.

b. Whenever NIST enters into a non-disclosure agreement, it tries to put limits on what is considered to be proprietary information. For example, the following types of information are often defined as not being proprietary:

- (1) Is in NIST's possession before receipt from the discloser;
- (2) Is or becomes a matter of public knowledge through no fault of NIST;
- (3) Is received by NIST from a third party without a duty of confidentiality;
- (4) Is disclosed by the discloser to a third party without a duty of confidentiality on the third party;
- (5) Is independently disclosed by NIST with the discloser's prior written approval; or

(6) Is developed independently by NIST without reference to the information disclosed under the Non-Disclosure Agreement.

5.06.07

APPROVAL PROCEDURES

a. The NIST Non-Disclosure Agreement for Receipt of Proprietary Information is available from the NIST Deputy Chief Counsel. If a Non-Disclosure Agreement other than the NIST model Non-Disclosure Agreement is used, the NIST Deputy Chief Counsel must approve before signature.

b. The NIST party(ies) desiring to receive proprietary information from an external party requests two copies of the NIST Non-Disclosure Agreement for Receipt of Proprietary Information from the NIST Deputy Chief Counsel, completes the information requested, and signs both copies in the space provided. All NIST recipients must sign the Agreement.

c. The Non-Disclosure Agreements are sent by the NIST party(ies) desiring to receive the proprietary information first to their OU Director through their division chief, along with a memorandum answering the "Due Diligence" questions below:

(1) The name of the organization disclosing the confidential information to NIST.

(2) A description of the subject matter to be disclosed with an explanation of why the owner of the information wishes to disclose it to NIST. Also, a description of why it is in the best interest of NIST to receive the proprietary information.

(3) The impact or consequences if NIST decides not to receive the proprietary information.

(4) Whether or not the proprietary information is related to a CRADA.

(5) A statement whether the proprietary information relates to any NIST-owned invention that has not yet been publicly disclosed or a NIST-owned invention that has been disclosed but not yet filed with the U.S. Patent and Trademark Office.

(6) The names of the NIST recipients. No non-NIST employee shall have access to proprietary information without the prior written approval of the NIST Deputy Chief Counsel.

(7) The proposed date of the requested disclosure.

(8) A statement as to whether the standard NIST Non-Disclosure Agreement will be used or one provided by the discloser. If the latter, provide written clearance from the NIST Deputy Chief Counsel.

d. The OU Director reviews and signs each non-disclosure Agreement and ensures that the conditions specified herein for use of the Agreement are met.

e. The OU Director sends both copies of the Agreement for signature to the organization providing the proprietary information with instructions to return one fully signed copy.

f. The OU Director sends that copy to the NIST Deputy Chief Counsel and copies are retained by the OU Director, the Chief of the Industrial Partnerships Program, and the recipients of the proprietary information.

g. The division chief retains custody of the disclosed proprietary information which is held under lock and key when not in actual use.

TREATMENT OF NIST's PROPRIETARY INFORMATION

Sections

5.07.01 Purpose

5.07.02 Scope

5.07.03 Policy

5.07.04 Legal Authority

5.07.05 Conditions for Use

5.07.06 Approval Procedures

5.07.01

PURPOSE

This subchapter states the policies and procedures for the disclosure of NIST's proprietary information via a Non-Disclosure Agreement. The purpose is to preserve NIST's ability to pursue patent protection on inventions by NIST employees when they are disclosing information upon which NIST may file for a patent.

5.07.02

SCOPE

This subchapter applies to all NIST employees.

5.07.03

POLICY

a. The vast majority of information and data developed by NIST is public domain at the time of its development. NIST does not have "trade secrets" that need to be protected. However, it may be advantageous to NIST's mission to patent the technology. Accordingly, NIST may want to avoid public disclosure of information on intramural inventions until such inventions are filed in the U.S. Patent and Trademark Office.

b. If such a disclosure is made, NIST promptly issues a non-enabling public announcement to comply with the statutorily-required competitive process for licensing NIST technology. The non-enabling public announcement, prepared by the Industrial Partnerships Program (IPP), provides a general understanding of the nature of the invention without revealing enough information for someone else to practice or duplicate it. That public announcement is made to ensure fairness in accessing NIST technology. It is NIST policy to avoid the preselection, or the appearance of preselection, by NIST employees of the private sector recipient of information on a NIST invention.

c. Disclosure of information developed under a Cooperative Research and Development Agreement (CRADA) may be restricted for a limited time, as specified by the terms of

the CRADA.

5.07.04

LEGAL AUTHORITY

35 U.S.C. 205

5.07.05

CONDITIONS FOR USE

a. Use the NIST Non-Disclosure Agreement to preserve NIST's ability to pursue patent protection on an intramural NIST invention upon which NIST may file for a patent. This would apply when:

(1) NIST employees are disclosing information that is patentable subject matter to non-U.S. government parties;

(2) They are contemplating the submission of an invention disclosure;

(3) During the time the IPP is evaluating an intramural invention; or

(4) After the OU Director has agreed that patent protection should be sought on an intramural invention but the Patent Application has not yet been filed with the Patent and Trademark Office.

b. CRADA project team members do not need a separate Non-Disclosure Agreement to disclose information on CRADA-related inventions to the CRADA partner. The CRADA already provides for the protection of such information.

5.07.06

APPROVAL AND RESPONSIBILITIES

a. The NIST party desiring to disclose the information obtains copies of the "Disclosure of NIST's Confidential Information" agreement and answers the following "Due Diligence" questions:

(1) Name of NIST discloser:

(2) Why is this disclosure an important next in the R&D plan?

Have talks been held with the Industrial Partnerships Program to determine the potential impact of this disclosure on subsequent patent protection?

(3) Describe the subject to be disclosed:

(4) Has this information been previously disclosed?

If so, what was disclosed? How? To whom? For what purpose? When?

(5) Proposed date for this requested disclosure:

(6) Identify the source of the information to be disclosed:

Is this information related to a CRADA?

Is this information related to a NIST invention not yet disclosed? Disclosed via an invention disclosure but not yet filed with the U.S. Patent and Trademark Office?

(7) NIST will disclose the information to:

_____ (Person within the Receiving Organization)

_____ (Organization)

(8) NIST will place a disclosure ("non-enabling") in a public media. Identify the media to be used (more than one may be used):

_____ Commerce Business Daily

_____ Federal Register

_____ Trade journal (identify _____)

b. The IPP representative for the appropriate OU Director assists in responding to these questions. The responses provide the OU Director with detailed information on circumstances of the planned disclosure. IPP arranges for any required non-enabling public announcement.

c. The responses to the "Due Diligence" questions and the Non-Disclosure Agreement are routed to the OU Director. The OU Director reviews and approves each Non-Disclosure Agreement and ensures that the conditions specified herein for use of the Agreement are met.

d. The signed Non-Disclosure Agreement is sent by the OU Director to the Chief of the IPP for signature along with the responses to the "Due Diligence" questions.

e. The IPP sends two copies of the Non-Disclosure Agreement to the party receiving the information for signature along with instructions to return one of the signed originals. IPP retains the signed original and distributes copies to the NIST discloser and the OU Director.

NIST COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENT PROGRAM

Sections

5.08.01 Purpose

5.08.02 Scope

5.08.03 Policy

5.08.04 Legal Authority

5.08.05 Conditions for Using CRADAs

5.08.06 Approvals and Responsibilities

5.08.01

PURPOSE

This subchapter states the policies and procedures to be followed in the NIST Cooperative Research and Development Agreement Program (CRADA).

5.08.02

SCOPE

This subchapter applies to all NIST employees.

5.08.03

POLICY

a. NIST strongly encourages collaborative R&D efforts with organizations on relevant and important mission activities. As part of the Cooperative Research and Development Program, NIST may work with for-profit organizations, nonprofit organizations (including universities), public and private foundations, state and local governments, and individuals on joint R&D projects of mutual interest. A CRADA must have at least one non-federal partner.

b. NIST considers assistance to industry and cooperative research and development activity as part of the employee's official duties. NIST employees are not permitted to consult on their own behalf, for personal or financial gain, in areas related to the scope of their official duties and technical activities at NIST.

c. CRADA partners may provide funds, personnel, equipment, services, and property to a CRADA. NIST may contribute employees, equipment, services, and funds (no funds to a non-federal partner) to a CRADA.

d. NIST believes that U.S. industry needs open access to NIST technical information. As a result, NIST emphasizes publication of its research results. Yet, NIST also recognizes that its CRADA partners may desire to gain competitive advantage from NIST research investments. Prospective partners should explicitly discuss their needs for delaying publication and protecting research results with NIST.

e. NIST desires that economic benefit of its research efforts flow to the U.S. economy. Accordingly, products from CRADA inventions for sale or use in the U.S. must be manufactured substantially in the U.S.

f. For CRADA and intramural inventions, NIST will grant patent licenses in return for royalties and other considerations. NIST's objective is to structure the licenses to encourage commercial use of the technologies, and thus, NIST will negotiate royalty rates and other terms that are reasonable under the circumstances. CRADA licenses will be royalty bearing, including Advanced Technology Program CRADAs where possible.

g. Non-NIST employees, such as Guest Researchers, shall not participate in NIST CRADAs unless 'by exception' as authorized in writing by the OU Director, CRADA partners, and the NIST Deputy Chief Counsel. If so authorized, the non-NIST employee must have a written agreement with NIST that details their CRADA obligations.

5.08.04

LEGAL AUTHORITY

15 U.S.C. 3710a, as amended

5.08.05

CONDITIONS FOR USING CRADAs

A CRADA must be compatible with the NIST mission; present no conflict of interest for NIST or its research project staff; and be acceptable to NIST approval authorities.

5.08.06

APPROVALS AND RESPONSIBILITIES

The OU Director, the NIST Deputy Chief Counsel, and the Chief of the Industrial Partnerships Program are signatories to the CRADA.

a. The NIST Principal Investigator and division submits an approval memorandum with the research plan to their management chain for approval.

b. The OU Director/Division Chief reviews the proposed activity and, if approved, forwards the approval memorandum to the Chief of the Industrial Partnerships Program for implementation.

c. The Industrial Partnerships Program manages the CRADA Program and prepares and transmits execution copies of the standard NIST CRADA to the firm; negotiates and obtains approval of modifications; and maintains the data base and permanent records of agreements.

d. The NIST Deputy Chief Counsel provides legal advice and review of NIST CRADAs including changes to the model CRADA.

INVENTIONS AND PATENTS

Sections

5.09.01 Purpose

5.09.02 Scope

5.09.03 Policy

5.09.04 Responsibilities

5.09.05 Protecting the Confidentiality of Invention Disclosures

5.09.06 Patent Ownership

5.09.07 Conflict of Interest

5.09.08 Invention Awards

5.09.01

PURPOSE

This subchapter states the NIST policy and procedures for pursuing patent protection of NIST inventions.

5.09.02

SCOPE

This subchapter applies to inventions made by all NIST employees at all NIST sites.

5.09.03

POLICY

a. Policy for NIST filing of Provisional Patent Applications:

NIST may file Provisional Patent Applications to preserve intellectual property rights while Invention disclosures are being processed.

b) Policy for NIST filing of Patent Applications:

In support of the NIST Mission *to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology – in ways that enhance economic security and improve the quality of life*, NIST encourages patent protection on an invention that

has been assigned to NIST by one or more inventors, when a patent would fulfill at least one of the following:

- (1) Increase the potential for current or future commercialization or use of the technology;
- (2) Have a positive impact on a new field of science or technology and/or the visibility and vitality of NIST; or
- (3) Further the goals of a Cooperative Research and Development Agreement (CRADA) or other agreement.

5.09.04

RESPONSIBILITIES

a. Employees - NIST researchers are responsible for recording and keeping all laboratory data. An employee who has made an invention should chronologically record the conception (idea) of the invention, the steps taken towards reducing the invention to practice, and the actual reduction to practice. Entries should be made in ink in a bound notebook, with each page signed and dated by the inventor and two coworkers indicating that they have read and understand the information. Separate charts, test set-ups and procedures, and data such as describing the reduction to practice, should be labeled, dated, and pasted or otherwise referenced in the notebook. These records are important and enable the government to establish the priority of the invention.

Employees are also responsible for:

- (1) Disclosing all inventions by completing and submitting the NIST Invention Information Sheet. Employees are responsible for reporting all their inventions, whether or not related to their work, so that the employees' and the government's rights in the inventions may be determined;
- (2) Cooperating with the activities of the Office of Technology Partnerships (OTP) and the Patent Review Committee (PRC) in the determination as to whether or not NIST should seek patent protection;
- (3) Working with the Patent Attorney retained by the OTP to prepare and prosecute a patent application, should one be filed; and
- (4) Providing reasonable assistance in assisting a licensee in the commercialization of the technology.

b. Supervisors - Responsible for ensuring that employees keep appropriate records of their scientific activities and report inventions through the Operating Unit (OU) management chain to the OTP. Once a patent application has been filed, Supervisors are responsible for maintaining careful oversight of the inventor's further research, development, or collaborations involving the technology and participation in the dissemination of information on the invention.

c. OU Directors/Division Chiefs - Responsible for reviewing, and providing written comments on, as appropriate, and forwarding all submitted invention disclosures to the OTP. With input from the PRC, the OU Director makes the final decision on whether or not to seek patent protection.

d. Office of Technology Partnerships (OTP) - OTP manages the Patent Program and is responsible for assessing invention disclosures, chairing the PRC, preparing and submitting the PRC's recommendations on whether or not to seek patent protection to the OU Director, and guiding NIST inventions through the patenting process. As appropriate to a specific disclosure, OTP (i) conducts a preliminary prior art search, (ii) interacts with the inventors, industry, and parties claiming co-ownership rights, and (iii) works with the Office of NIST Counsel to develop information for the PRC to use in its assessment. If following the commercial assessment of the invention, NIST decides to pursue patent protection, OTP: coordinates the patenting process, procures law firm assistance, provides general patent process information for NIST scientists, and negotiates licensing of patented technology. (See Subchapter 5.10, Licensing NIST Inventions.)

e. Office of NIST Counsel - Makes inventor rights determinations, performs legal review of the patenting process, and serves as an ex-officio member of the PRC.

f. Patent Review Committee (PRC) - The PRC is responsible for reviewing the invention disclosure, information provided by OTP, the NIST Counsel's Office, and such expert opinion as may be solicited, and providing a recommendation to the OU Director submitting the disclosure on whether or not NIST should seek patent protection.

The PRC is chaired by the CRADA and Licensing Officer from OTP responsible for a specific disclosure. The committee consists of (a) one standing member nominated by each of the Laboratory OU directors and (b) up to two individuals with technical expertise in the field of a specific disclosure nominated by the OU director submitting the disclosure. The Director of Technology Services may nominate one non-NIST member. The NIST Counsel and the Chief of OTP are ex-officio members of the Committee. A quorum will be met when the chair and at least half of the standing members and the technical experts are present, including individuals participating via teleconference or videoconference. Decisions as to whether or not to recommend to the OU Director that NIST seek patent protection are made by majority vote of the voting members taking part in the meeting.

5.09.05

PROTECTING THE CONFIDENTIALITY OF INVENTION DISCLOSURES

If the inventor has submitted or plans to submit an invention disclosure, they should not contact companies or anyone else outside of NIST concerning the invention without first discussing the consequences of the proposed contacts with the OTP or with the NIST Counsel's Office. NIST may be obligated to keep the invention confidential or the invention may contain proprietary information that NIST is obligated to keep confidential.

5.09.06

PATENT OWNERSHIP

NIST Inventors shall take prompt action to report inventions directly related to the inventor's official duties, made during working hours or with the contribution of Government facilities, equipment, materials, funds, information or with the time or services of other Government employees on official duty. To ensure that their inventions are protected in a timely manner, inventors shall submit a completed DN-45, NIST Invention Disclosure Form (IDF), as soon as there is enough information to evaluate the invention. Waiting to submit an IDF until a publication is cleared by WERB or BERB may adversely affect the ability of NIST to protect the invention.

NIST abides by government regulations, policies and procedures when making an invention Rights Determination. Under Federal Regulation, there is a presumption that the U.S. Government is entitled to own work-related inventions made by NIST scientists using government resources. It is the decision of NIST, not individual scientists, as to when and how NIST owned inventions are to be commercialized.

NIST will file for patent protection in accordance with the NIST Patent Policy.

Commercialization of technologies created by NIST employees may be accomplished through various methods including, when appropriate, patenting and licensing. Determinations of government ownership made by NIST are appealable by employee-inventors and, in cases where the government decides not to obtain title to an invention for the purpose of patenting, or not to pursue other commercialization mechanisms including publication, the Government leaves title with the employee inventors, subject to a Government use license.

5.09.07

CONFLICT OF INTEREST

As federal employees, inventors must not enter into situations that create a conflict of interest. NIST inventors should contact the NIST Department of Commerce Ethics Office at (202) 482-5384 if they have questions as to what they personally may do with their inventions.

5.09.08

INVENTION AWARDS

A federal employee assigning their rights to NIST as the inventor is entitled to receive a portion of the royalty and other payments received through license agreements. Statute requires that the inventor(s) annually receives the first \$2,000 and at least 15 percent (NIST policy is 30 percent) of any license income over and above that amount, with total annual limit of \$150,000.

LICENSING NIST INVENTIONS

Sections

5.10.01 Purpose

5.10.02 Scope

5.10.03 Policy

5.10.04 Legal Authorities

5.10.05 Conditions for Licensing

5.10.06 Audits Requested by NIST

5.10.07 Approvals and Responsibilities

5.10.01

PURPOSE

This subchapter states the policies and procedures to be followed in licensing NIST inventions. NIST License Agreements are the vehicles by which NIST's intellectual property rights in patented (or patentable) technology are made available to industry. Inventions may arise from intramural, CRADA, or other collaborative research, and may be wholly or partially owned by NIST. The licenses may provide exclusive, coexclusive or nonexclusive rights, and may be defined by duration, field of use, and geography.

5.10.02

SCOPE

This subchapter applies to all NIST employees.

5.10.03

POLICY

a. Intramural Inventions - Applying for, obtaining a patent on, and licensing NIST intramural inventions is one of many routes by which NIST helps achieve industry's use of NIST technology. When the OU Director has agreed that patent licensing is the appropriate route in a given situation, it is NIST policy to strike a balance:

- (1) Between the need to provide fair and equal access to the technology, and getting the technology rapidly to industry;
- (2) Between negotiating licensing terms that provide industry with an incentive to commercialize the technology, and preserving the value of the technology through royalties; and
- (3) Between the need to get ongoing NIST research done, while also providing the continuing support to industry that may be necessary for the successful commercialization of the invention.

The availability of NIST intramural inventions must be publicly announced in the statutorily required manner. Statute also requires and provides the procedure for making a public announcement of NIST's intention to grant an exclusive license to NIST's ownership of an intramural invention. Objections received from the public to the proposed exclusive license must be taken into account by NIST.

b. CRADA Inventions - The standard NIST CRADA provides CRADA partners with an option to negotiate an exclusive field of use license to NIST's ownership in CRADA inventions. No public announcements are required for licensing CRADA inventions. In a CRADA with an ATP recipient on the subject of the ATP award, NIST provides title to all inventions, including those made by NIST, to the ATP CRADA partner in accordance with 15 U.S.C. 278n(d)(11)(A).

c. Royalties - Statute requires that the inventor(s) receives at least 15 percent (NIST policy is 30 percent) of any license royalties or other payments received up to \$150,000 annually, after the first \$2,000 of such payments go to the inventor(s).

5.10.04

LEGAL AUTHORITIES

35 U.S.C. 207

37 C.F.R. 404

15 U.S.C. 3710, as amended

15 U.S.C. 278n(d)(11)(A)

5.10.05

CONDITIONS FOR LICENSING

For licensing NIST inventions, an invention must be compatible with the NIST mission; present no conflict of interest for NIST or its research project staff; and be acceptable to NIST approval authorities.

5.10.06

AUDITS REQUESTED BY NIST

NIST reserves the right, at its discretion, to conduct an independent audit verifying reports and payments as stated in the license.

5.10.07

APPROVALS AND RESPONSIBILITIES

a. The OU Director, NIST Counsel, and Chief, OTP are all responsible for signing the license.

b. The Office of Technology Partnerships (OTP) is responsible for:

- Providing copies of the license agreement to the Finance Division.
- Preparing and sending letters to licensees and assignees requesting payments due under the license, with the licensee/assignee directed to send payments to the Finance Division.
- Monitoring receipt of required payments and royalty reports, following up with licensees/assignees when payments are not forthcoming and, in consultation with the Office of NIST Counsel, taking or recommending appropriate action, which may include license termination on delinquent accounts.
- Monitoring licensee performance in bringing the licensed technology to the point of 'practical application' per the license commercialization plan and other specific milestones included in the license.
- Providing licensees with a self-audit checklist when sending the executed copy of a license and at such other times as may be appropriate.
- Recommending to the appropriate OU Director when a license should be terminated and, in consultation with the Office of NIST Counsel, terminating licenses when the licensee has not, in NIST's judgment, exercised diligence in commercializing the licensed technology.
- Forwarding information regarding potential license infringement for the licensee, inventors, or others to the NIST Counsel.
- Maintaining a current relational database of all licenses and related information.
- Preparing the recommendations memorandum for the Director, Technology Services, for formal audit of licenses as appropriate.
- Requesting the Acquisitions and Logistics Division to issue a contract for approved audits and the Grants and Agreements Management Division to serve as the Audit Resolution Officer on such contracts. OTP will serve as the COTR for the contract.
- Preparing and sending letters to audited licensees requesting payment of any amounts determined by the audit to be due to NIST.

c. The Director, Technology Services is responsible for:

- Reviewing and, if appropriate, approving audit recommendations submitted by OTP. Requesting that funds to pay for the audit be provided from the overall license income received by NIST. If sufficient funds are unavailable for the audit from the overall license income received by NIST, but the Director, Technology Services, believes that a compelling justification for an audit exists, he/she may request, via justification memorandum through the Budget Division to the NIST Deputy Director, funds from another source.

d. The Budget Division is responsible for:

- Determining that there are sufficient funds, after royalty payments and other obligations taken from the licensing income, to pay for the audit are available from the license income received by

NIST and, in that case, approving or disapproving the request of the Director, Technology Services.

e. The Finance Division is responsible for:

- Receiving payments due from licensees and assignees.
- Providing the following to OTP in a timely manner: copies of all reports received from licensees/assignees; details of income received from all licensees/assignees, broken down into types of payments; details of the disbursement of license income, including royalties and other payments.
- Disbursing payments from licensees/assignees per NIST policy and statutory requirements.
- Maintaining a current database of all licenses/assignments, which incorporates details on payments and disbursements, and providing on-line, viewable access to the database to OTP.
- Collecting payments due NIST as determined by any audit.

f. The NIST Counsel is responsible for:

- Providing legal advice and guidance in the patent licensing and audit processes, including addressing and resolving pre- and post-licensing and auditing legal issues.
- Serving as the NIST lead in addressing legal disputes between NIST and its licensees, including patent infringements.
- Providing legal advice and consultation to OTP and other NIST offices prior to the initiation of an audit, license termination, or other action that may adversely affect a licensee's rights.

CONTRACT RESEARCH PERFORMED BY NIST FOR NON-FEDERAL PARTIES

Sections

5.12.01 Purpose and Scope

5.12.02 Policy

5.12.03 Legal Authorities

5.12.04 Conditions for Use

5.12.05 Approvals and Responsibilities

Appendix A – Amendment to Purchase Order with NIST

5.12.01

PURPOSE AND SCOPE

This subchapter states the policies and procedures to be followed when NIST employees perform research under contract for a non-federal party. This subchapter does not apply to calibration services.

For purposes of this subchapter, contract research is defined as mission-appropriate, non-collaborative technical work performed by NIST using NIST employees or facilities funded in whole or in part by a non-federal entity.

5.12.02

POLICY

NIST may provide research services under contract to non-federal parties under certain circumstances and conditions, as stated below.

NIST may use a contract when the research is non-collaborative, and conforms to the circumstances and conditions below.

NIST will own all intellectual property that results from the contract research and NIST is free to place all research results in the public domain. If the non-federal party wishes to own the results of the contract research, keep research results proprietary, or have the research performed collaboratively with NIST, then the non-federal party should use a Cooperative Research and Development Agreement (CRADA) or a Facility-Use Agreement.

5.12.03

LEGAL AUTHORITIES

15 U.S.C. 275a

15 U.S.C. 277

15 U.S.C. 278b(e)
15 C.F.R. 200

5.12.04

CONDITIONS FOR USE

NIST may conduct contract research for others when:

a. **One (1) or more** of the following circumstances exists:

- (1) acceptance by NIST establishes traceability of measurements to national standards;
- (2) the private sector cannot or will not develop test methods for materials, mechanisms, or structures related to items purchased by the government or important to the public interest;
- (3) requirements for accuracy of physical constants and properties of materials cannot be met by other sources;
- (4) there is a unique capability of NIST required; and/or
- (5) use of a private sector source could cause significant and intolerable delays in providing services and results; and

b. **All** of the following conditions are met:

- (1) consistent with and complementary to the NIST mission;
- (2) provides benefit to the laboratory's technology base, core competence, technical capabilities;
- (3) would not place the NIST facility in direct competition with the private sector;
- (4) consistent with environmental, safety, and health requirements;
- (5) consistent with acceptable standards for humane treatment of human and animal subjects involved in research or other activities of the government; and,
- (6) the research activity does not compromise or create the appearance of compromising NIST's third party objectivity.

The contract must include the standard NIST clauses on publication, intellectual property rights (NIST owns exclusively), treatment of proprietary information, indemnification and liability, and the use of NIST's name. These are contained in the standard "Amendment to Purchase Order with National Institute of Standards and Technology" which is included as Appendix A to this subchapter. Any variations from these

provisions must be approved by the NIST Deputy Chief Counsel.

5.12.05

APPROVALS AND RESPONSIBILITIES

a. The OU ensures that an acceptable purchase order from a non-federal party for NIST contract research conforms to the above Conditions for Use, and that it is consistent with the "Amendment to Purchase Order with National Institute of Standards and Technology" a sample of which is included as Appendix A to this subchapter.

b. The OU Director or designee approves, disapproves, or renegotiates the purchase order proposed by the sponsoring party.

c. The Comptroller approves purchase orders for contract research over \$25,000, and sends to the NIST Deputy Chief Counsel if the purchase order does not conform to the terms of the above-mentioned "Amendment" or if NIST and the sponsoring party need help in negotiating terms.

d. The NIST Deputy Chief Counsel approves non-standard (NIST) contract terms and assists in negotiating contracts.

Chapter 5 – Technology Support

Subchapter 5.16 Traceability

Sections

5.16.01 Purpose

5.16.02 Background

5.16.03 Scope

5.16.04 Legal Authority

5.16.05 Policy

5.16.06 Delegations of Authority

5.16.07 Supplementary Information

5.16.08 Responsibilities

5.16.09 Content Owner

5.16.10 Effective Dates

5.16.01

PURPOSE

This Subchapter describes the NIST Policy on Metrological Traceability.

5.16.02

BACKGROUND

a. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. To help meet the measurement and standards needs of U.S. industry and the nation, NIST provides calibrations, standard reference materials, standard reference data, test methods, proficiency evaluation materials, measurement quality assurance programs, and laboratory accreditation services that assist a customer in establishing traceability of measurement results.

b. Metrological traceability requires the establishment of an unbroken chain of calibrations to specified references. NIST assures the traceability of measurement results that NIST itself provides, either directly or through an official NIST program or collaboration. Other organizations are responsible for establishing the traceability of their own results to those of NIST or other specified references. NIST has adopted this policy statement to document the NIST role with respect to traceability.

5.16.03

SCOPE

This subchapter is applicable to all NIST employees at Gaithersburg and Boulder.

5.16.04

LEGAL AUTHORITY

15 U.S.C. 272(b) and (c)

5.16.05

POLICY

To support the conduct of its mission and to ensure that the use of its name, products, and services is consistent with its authority and responsibility, NIST:

- a. Adopts for its own use and recommends for use by others the definition of metrological traceability provided in the most recent version of the International vocabulary of metrology: "property of a measurement result whereby the result can be related to a reference through a documented unbroken chain of calibrations, each contributing to the measurement uncertainty." (International Vocabulary of Metrology – Basic and General Concepts and Associated Terms, VIM, 3rd edition, JCGM 200:2008, also published as ISO Guide 99 by ISO (ISO/IEC Guide 99-12:2007, International Vocabulary of Metrology – Basic and General Concepts and Associated Terms, VIM (2008).)
- b. Establishes metrological traceability of the results of its own measurements and of results provided to customers in NIST calibration and measurement certificates, operating in accordance with the NIST Quality System for Measurement Services. See Subchapter 5.17 and access the following website: <http://www.nist.gov/nistsystem/>.
- c. Asserts that providing support for a claim of metrological traceability of the result of a measurement is the responsibility of the provider of that result, whether that provider is NIST or another organization; and that assessing the validity of such a claim is the responsibility of the user of that result.
- d. 4. Communicates, especially where claims expressing or implying the contrary are made, that NIST does not define, specify, assure, or certify metrological traceability of the results of measurements except those that NIST itself provides, either directly or through an official NIST program or collaboration. See also NIST Administrative Manual, Subchapter 5.03, NIST Policy on Use of its Name in Advertising and the following website: <http://www.nist.gov/traceability/503.htm/>.
- e. Collaborates on development of standard definitions, interpretations, and recommended practices with organizations that have authority and responsibility for variously defining, specifying, assuring, or certifying metrological traceability.

f. Develops and disseminates technical information on traceability and conducts coordinated outreach programs on issues of metrological traceability and related requirements.

5.16.06

DELEGATIONS OF AUTHORITY

The oversight of implementation of the NIST policy on metrological traceability is assigned to the NIST Measurement Services Advisory Group (MSAG).

5.16.07

SUPPLEMENTARY INFORMATION

For definitions of key terms in the statement of policy and other supplementary information.

5.16.08

RESPONSIBILITIES

a. NIST staff is responsible for disseminating advice on metrological traceability to customers and stakeholders as defined in this subchapter.

b. MSAG is responsible for oversight of implementation of the NIST policy on metrological traceability.

5.16.09

CONTENT OWNER

The Chief of the Measurement Services Division is responsible for maintaining this Subchapter.

5.16.10

EFFECTIVE DATE

a. August 12, 2009

NIST Trademark Protection

5.22.01 Purpose

5.22.02 Scope

5.22.03 Policy

5.22.04 Responsibilities

5.22.01 Purpose

This subchapter states the NIST policy and procedures for Trademark Protection.

5.22.01 Scope

This subchapter applies to all registered NIST Trademarks.

5.22.03 Policy

NIST will register trademarks when requested by the relevant OU Director, or the Chief of Staff if originating from the NIST Director's Office, when doing so will support the NIST Mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology – in ways that enhance economic security and improve the quality of life.

5.22.04 Responsibilities

- a) NIST Employees are responsible for submitting all requests for Trademark registration, Trademark enforcement or any other NIST Trademark matter through their management chain to the Deputy Director of Technology Services.
- b) OU Directors, or the Chief of Staff for requests originating in the NIST Director's office, are responsible for reviewing and approving all requests for Trademark registration, Trademark enforcement or any other NIST Trademark matter sent to the Deputy Director of Technology Services.
- c) Deputy Director of Technology Services (DDTS) shall be the sole coordinating office for all Trademark matters with the Chief, General Law Division (GLD), of the Department of Commerce. Upon receipt of a request for a new Trademark or other Trademark-related action, the DDTS will review as appropriate with the Office of NIST Counsel (ONC), the General Law Division (GLD), and the Office of Public and Business Affairs (PBA), and if appropriate will cause a Trademark search to be conducted.

Depending on the results of the search and the consultations with ONC, PBA, and

Trademark counsel, Office of Technology Partnership (OTP) will either request that a Trademark application be filed by GLD or work with the initiator, PBA, and ONC to attempt resolve any issues.

d) OTP will develop and maintain a database of NIST Trademarks, including required renewal dates and fees, with assistance from the ONC and GLD.

Procedures for NIST Employees in a National Emergency

Sections

6.01.01 Purpose

6.01.02 Scope

6.01.03 Legal Authority

6.01.04 Policy

6.01.05 Delegations of Authority

6.01.06 Responsibilities

6.01.07 Procedures

6.01.08 Content Owner

6.01.09 Effective Dates

6.01.01

PURPOSE

This subchapter outlines the emergency actions to be taken by NIST employees in the event of declaration of a national emergency, such as an attack upon the country that is either imminent or under way.

6.01.02

SCOPE

The procedures in this subchapter apply to NIST employees.

6.01.03

LEGAL AUTHORITY

Executive Order 12656, Assignment of Emergency Preparedness Responsibilities.

6.01.04

POLICY

NIST must, in the event of a national emergency, take prudent measures to ensure, to the maximum extent possible, the safety of NIST employees, whether they are in the United States or abroad.

6.01.05

DELEGATIONS OF AUTHORITY

The NIST Director hereby delegates to the Director of NIST Boulder Laboratories the authority to provide local direction to NIST employees located in Boulder and Fort Collins, Colorado and Kauai, Hawaii.

6.01.06

RESPONSIBILITIES

a. The NIST Director:

- (1) Ensures that NIST establishes and maintains an effective all-hazards emergency preparedness program and Continuity of Operations (COOP) Plan.
- (2) Directs the NIST Emergency Coordinator in developing and activating the NIST COOP Plan.

b. The NIST Deputy Director oversees the NIST emergency management program.

6.01.07

PROCEDURES

a. NIST Employees in the United States:

(1) Employees on duty at NIST facilities in Gaithersburg, Maryland; Boulder and Fort Collins, Colorado; and Kauai, Hawaii shall, upon receiving the announcement of a national emergency, remain on duty until instructed by NIST management to either:

- (a) return home,
- (b) take shelter at the facility, or
- (3) report to an alternate location.

(2) Employees on duty at non-NIST locations shall, upon receiving the announcement of a national emergency, comply with emergency instructions announced by local authorities.

(3) Designated Emergency Employees who are off duty are to report to their regular duty station or to their pre-designated emergency assignment as soon as circumstances permit.

(4) NIST employees who are off duty, on leave or on temporary duty and unable to report to their regular duty station or their assigned relocation site are to

comply with emergency instructions announced by local authorities. They are encouraged to contact their NIST supervisors for instructions as soon as circumstances permit.

(5) In the event NIST employees cannot contact their supervisors they should check the NIST Status Line:

(a) Gaithersburg—Call 301-975-8000 or 1-800-437-4385, extension 8000;

(b) Boulder—Call 303-497-4249. (Press 4 for Gaithersburg information.)

b. NIST Employees Located in a Foreign Country:

(1) NIST employees abroad on official travel, training, leave, etc., who learn of, or are notified of, an attack upon the United States, its territories, the host country, or any other country friendly to the United States, should immediately contact the nearest U.S. foreign service post for guidance and instructions.

(2) NIST employees abroad should work with Department of State officials to ensure that the Department of Commerce has been notified of their individual and family status at the time of the emergency. They are encouraged to contact their NIST supervisors as soon as circumstances permit.

(3) If an employee and their dependents have been evacuated to a foreign safe haven, they should ensure that this information has been reported to the Department of Commerce.

6.01.08

Content Owner

190 – Chief Facilities Management Officer

191 – Emergency Services Division

6.01.09

Effective Date

June 30, 2009

FIRE PROTECTION PROGRAM

Sections

6.05.01 Purpose

6.05.02 Scope

6.05.03 Legal Authority

6.05.04 Policy

6.05.05 Delegations of Authority

6.05.06 Responsibilities

6.05.07 Content Owner

6.05.08 Effective Dates

Appendix A - Installation and Use of Heat Producing Staff-Owned Electrical Appliances

Appendix B - Excess Property and Hallway Storage

6.05.01 PURPOSE

This subchapter details NIST's internal policy and procedures for a comprehensive fire prevention and protection program.

6.05.02 SCOPE

The fire prevention and protection program applies to all individuals, activities and operations at NIST sites.

6.05.03 LEGAL AUTHORITIES

Department Organization Order 30-2A
Department Organization Order 30-2B

6.05.04 POLICY

NIST will ensure effective fire prevention and protection program is present at all NIST sites to reduce loss of life and property from fire.

6.05.05 Delegation of Authority

- a. At Gaithersburg, Maryland the NIST Director has delegated authority for fire prevention, protection and emergency medical services through the Chief Facilities Management Officer (CFMO) to the Chief, Emergency Services Division.
- b. At Boulder and Fort Collins, Colorado, and Kauai, Hawaii, the NIST Director has delegated authority for fire prevention and protection coordination to the Site Manager, NIST Boulder Laboratories.

6.05.06 RESPONSIBILITIES

- a. Each NIST employee, associate and contractor is responsible for ensuring that their activities are conducted in a safe manner that minimizes the risk of accidental fire.
- b. Division chiefs and group leaders are responsible for ensuring that employees and associates within their organizations follow the requirements of Appendix A and Appendix B.
- c. At Gaithersburg, the Fire Protection Group, Emergency Services Division (CFMO), is responsible for:
 - (1) Reducing or eliminating lost production time and resources through identification and correction/control of potential fire hazard conditions;
 - (2) Developing and maintaining fire prevention regulations and disseminating this information by regular or special bulletins or through the implementation of a fire safety education program;
 - (3) Testing fire alarm, detection, and suppression systems;
 - (4) Issuing work permits for activities having high accidental fire potential and appliance permits for heat producing employee-owned appliances;
 - (5) Inspecting and testing fire hydrants and fire protection water supply systems;
 - (6) Providing consultation with NIST managers, employees and associates in matters regarding fire safety;

- (7) Providing portable hand-held fire extinguisher training and conducting evacuation drills;
- (8) Establishing fire safety policies, procedures, and requirements based on the National Fire Protection Association fire codes, local codes and regulations, and DoC regulations;
- (9) Responding to all emergency calls regarding fire, first aid/ambulance, and chemical spills and odors, as well as service calls such as water leaks;
- (10) Providing atmospheric testing for confined space entries on an emergency basis or in the absence of the Plant Safety Representative or NIST Safety Office Representative;

Note:

A confined space is any space: 1) that has limited or restricted means of entry or exit; 2) is large enough for a person to enter to perform tasks; 3) and is not designed or configured for continuous occupancy (e.g., a utility tunnel, the inside of a fluid storage tank, a septic tank that has contained sewage, and a small underground electrical vault). Confined spaces that present special hazards to workers, including risks of toxic or asphyxiant gas accumulation, fires, falls, flooding, and entrapment may be classified as permit-required confined spaces depending on the nature and severity of the hazard. In Gaithersburg, contractors are responsible for their own Confined Space Entry Program, to include: a) their own entry permit process; b) Monitoring the space before entering, and while a person is in the space; c) providing their own equipment – monitoring equipment, retrieval equipment, exhaust blowers, etc; and d) proof of confined space entry training.

- (11) Reducing or eliminating temporary storage in hallways, etc., which could be potentially hazardous in the event of an emergency;
- (12) Evaluating requests for temporary storage in hallways or other areas which may impede employees from evacuating during emergencies and making recommendations to ensure maximum safety for employees and fire suppression personnel;
- (13) Providing fire service personnel at Gaithersburg that are certified as Fire Fighters, Emergency Medical Technicians(EMT)-A, EMT-B, and Hazardous Material Technicians as prescribed by the State of Maryland;
- (14) Insuring NIST complies with applicable fire codes;
- (15) Suggesting improvements for detection systems and suppression materials; and
- (16) Maintaining a Fire Protection Group hazardous materials data base to be used during emergencies.

c. At Boulder:

- (1) The Site Manager, and the Office of Safety, Health and Environment are responsible for ensuring that the fire prevention and protection and the emergency medical care programs function effectively. This includes:
 - (a) Developing, implementing, and monitoring the fire prevention and protection and the emergency medical care program;
 - (b) Reviewing and evaluating the effectiveness of the program and making changes where required to negate new or unique potential fire hazards;
 - (c) Utilizing staff resources, supplies, and equipment to ensure maximum efficiency and effectiveness;
 - (d) Promoting the concepts of fire safety and prevention and developing educational techniques for the dissemination of fire safety information;
 - (e) Identifying confined spaces and enumerating the associated hazards, and providing initial or pre-entry and periodic atmospheric testing for confined space entries in compliance with applicable regulations, including but not limited to 29 CFR 1910.146;

Note: In Boulder, NIST may provide pre-entry monitoring for contractors entering confined spaces on NIST controlled property; however, the contractors are responsible for their own Confined Space Entry Program, including monitoring.
--

- (f) Providing liaison with local fire protection and emergency medical services; and
 - (g) Cooperating with local fire protection services to develop and maintain fire plans for effective response to emergencies.
 - (2) The Chief, Engineering, Maintenance and Support Services, in coordination with the Site Manager, and the Safety, Health and Environment Division has the responsibility for the maintenance and operation of the fire prevention system, including regular testing of fire alarm, detection, and suppression systems

6.05.07

CONTENT OWNER

Chief, Emergency Services Office

6.05.08

EFFECTIVE DATE

August 31, 2009

APPENDIX A

INSTALLATION AND USE OF HEAT PRODUCING STAFF-OWNED ELECTRICAL APPLIANCES

This appendix establishes a procedure for the installation, control and approval of heat producing staff (employee and associate) - owned electrical appliances. For purposes of this appendix, heat producing staff-owned electrical appliances include items such as microwave ovens, toasters, toaster ovens, hot plates, coffee makers, and portable space heaters.

1. Requirements - Staff-owned electrical appliances are not to be installed or used until the appliance and its location is approved by the Fire Protection Group (in Gaithersburg) or the Safety, Health and Environmental Division (in Boulder). Approval is contingent upon meeting the following requirements.
 - a. The electric circuit used to energize the appliance must be capable of handling the additional load.
 - b. The appliance must bear the label of Underwriters Laboratory or other recognized testing laboratory.
 - c. The appliance must be found free of defects upon inspection.
 - d. Hot plates and similar heat producing appliances must:
 - (1) Be equipped with a pilot light to indicate when the current is turned on;
 - (2) Have no obstructions within 36" of the front (to allow unimpeded movement to respond to a fire);
 - (3) Be placed on a non-combustible base such as a metal plate or a ceramic or formica countertop; and
 - (4) Have at least six (6) inches clearance from unprotected combustible materials on all sides and at least 36 inches overhead (from the top of the appliance).
 - e. Automatic electric coffee makers and similar automatic appliances must:
 - (1) Have enclosed heating elements;
 - (2) Be protected from combustibles as indicated in d. (3) and (4) above;
 - (3) Not be a "submersible-type" heater (these are not allowed);
 - (4) Be clearly in view and visible for ready inspections; and

- (5) Be equipped with an automatic shut-off feature.
- f. Attachment cords on appliances are not to exceed eight (8) feet in length and are not to be run in raceways, under rugs, within furniture, or through doorways or partitions.
- g. The use of extension cords is discouraged. When absolutely necessary, such cords are to be rated for at least 15 amp, 120-volt service. Under no circumstances are extension cords to be attached to other extension cords or power strips (daisy chaining). Requirements indicated for attachment cords (paragraph f.) also apply to extension cords.
- h. Attachment and extension cords must not be placed where they create a tripping hazard to occupants or visitors. Frayed or damaged cords are to be replaced.
- i. NIST does not encourage the use of electric space heaters, but recognizes that in some cases a local space heater is necessary for health and safety purposes.
 - (1) Staff shall refer to the manufacturer's instructions to see how far the heater should be placed from combustible materials, and for how far the heater should be placed from the floor so that carpeting or flooring materials don't ignite.
 - (2) Do not leave the heater operating unattended. Portable electric air heaters are designed for use only as temporary supplemental heating and only while attended.
 - (3) Ensure that clutter does not build up in the vicinity of the space heater.
- j. Appliances are to only be used for their intended purpose.

2. Responsibilities

- a. Staff members are responsible for requesting approval for their personally owned heat producing electrical equipment by the Fire Protection Group (in Gaithersburg) or the Safety Health and Environmental Division (in Boulder).
- b. Division Safety Representatives are responsible for:
 - (1) Assuring that all staff-owned electrical appliances installed and used have been approved by the Fire Protection Group (in Gaithersburg) or the Safety Health and Environmental Division (in Boulder).
 - (2) Directing use of unapproved appliances be discontinued and that they be removed from the facility.
 - (3) Reminding personnel using microwave ovens, toasters, toaster ovens, hot plates and space heaters that they are required to keep the appliance under

observation while actively in use. Coffee makers and similar devices with a low likelihood of burning items are exempt from the observation requirement.

- (4) Initiating an incident report for any fire alarms or smoke complaints associated with the permitted appliance.
- c. The Fire Protection Group (in Gaithersburg) or the Safety Health and Environmental Division (in Boulder) is responsible for:
 - (1) Processing approval requests for installation of staff-owned heat producing appliances;
 - (2) Inspecting the proposed appliance location for compliance with this directive;
 - (3) Considering the location of smoke detectors and other fire alarm sensors with respect to the proposed location;
 - (4) Verifying that the proposed appliance is approved by UL or another recognized testing laboratory;
 - (5) Attaching approval tag to all approved, staff-owned electrical appliances;
 - (6) Reviewing Incident Reports and taking appropriate action to resolve incident findings, including revocation of appliance permits; and
 - (7) Conducting annual follow-up inspections of approved, staff-owned electrical appliances to ensure compliance with requirements.

NIST reserves the final decision on any appliance or item determined to be inappropriate for facility use. Appliance permits will be revoked if appliances are involved in repeated fire alarms or incidents.

APPENDIX B

EXCESS PROPERTY AND HALLWAY STORAGE

Storage of excess property in hallways and receiving rooms is a hazard to building occupants and emergency services personnel when responding to an emergency. This appendix establishes a procedure for minimizing the hazards from excess property and hallway storage.

1. Requirements - Storage of furniture or equipment is not allowed in hallways or receiving rooms except when the Fire Protection Group (FPG) in Gaithersburg or the Safety, Health and Environmental Division in Boulder (SHED) has been informed (by telephone or e-mail) and has granted permission for the storage or the storage will be for less than eight hours.
 - a. When hallway or receiving room storage is permitted by the FPG/SHED, it is for a period of ten workdays or less. FPG/SHED will also issue a sign that must be posted stating that the storage is permitted.
 - b. Storage of large equipment and shipping containers in receiving rooms is allowed only when approved by both FPG/SHED and Excess Property (Administrative Services Division (ASD) in Gaithersburg and Engineering, Maintenance and Support Services Division (EMSS) in Boulder). The owner's name, room number, and organizational unit number must appear on all items.
 - c. When storage is permitted:
 - (1) The storage must be kept to one side of the hallway. In General Purpose Laboratories, storage must be put on the exterior (office) side of the building. Storage is forbidden against walls marked "No storage this side".
 - (2) There must be at least a three-foot clearance from the wall opposite the storage and the storage.
 - (3) The storage must not block exits, manual fire alarm stations, fire extinguishers, automatic external defibrillators, safety showers/eyewashes, or other life safety equipment that are located on the interior hallways.
 - (4) In a receiving room, the storage must not block exits, roll-up doors, cylinder storage racks, or fire department inspector's test valves.
 - d. Furniture or equipment to be picked up by Excess Property personnel must have a copy of Form NIST-6, Report of Excess Property, posted for FPG/SHED to review.
 - e. Furniture or equipment that has been placed in a hallway or receiving room without prior approval from FPG/SHED will be tagged. If unapproved items remain in the hallways or receiving room for more than twenty-four hours, the

division chief will be contacted and directed to make arrangements to move the items to a secure storage area. In the event of recurring violations, the division chief is expected to take administrative action as described in NIST Administrative Manual, Subchapter 10.11, Adverse Actions.

- f. Vending machines shall be placed only in those areas approved for vending machines by FPG/SHED.

2. Responsibilities

- a. The division chief/group leader is responsible for ensuring that:
 - (1) Storage in hallways is permissible and, when necessary, for making sure that FPG/SHED is notified and permission received before furniture or equipment is stored in hallways or receiving rooms.
 - (2) A completed Form NIST-6 is sent to Excess Property (ASD in Gaithersburg and EMSS in Boulder) in a timely manner for any furniture or equipment to be excessed. Upon receipt of Form NIST-6, excess furniture or equipment is generally picked up within five workdays.
 - (3) The Grounds and Service Support Group is scheduled to pick up large items.
 - (4) Periodic checks are made to ensure that hallway storage meets the requirements of 1c. above.
- b. The Grounds and Service Support Group is responsible for moving furniture to another location within five workdays.
- c. FPG/SHED is responsible for:
 - (1) Determining if excess furniture or equipment can be placed in hallways or receiving rooms;
 - (2) Inspecting hallways and receiving rooms for compliance with this procedure; and
 - (3) Evaluating hallways and receiving rooms where furniture or equipment is stored for compliance with this procedure.

<p>NOTE: NIST reserves the right to restrict storage of materials in hallways and along egress routes based on regulations and Life Safety codes.</p>

<p>U. S. DEPARTMENT OF COMMERCE NATIONAL BUREAU OF STANDARDS</p> <p>ADMINISTRATIVE MANUAL</p>	<p>Chapter 6 Emergency Operations</p>
	<p>Subchapter 6.06 Facility Shutdown Plan</p>

FACILITY SHUTDOWN DUE TO LAPSE OF APPROPRIATIONS

Sections

- 6.06.01 Purpose
- 6.06.02 Scope
- 6.06.03 Policy
- 6.06.04 Designation of Officials
- 6.06.05 Responsibilities
- 6.06.06 Funding
- 6.06.07 Duty Status of Employees
- 6.06.08 NBS Shutdown Operations
- Appendix A - Maximum Staff Levels During NBS Shutdown
- Appendix B - Some Effects of Furlough Status

6.06.01

PURPOSE

This subchapter provides general guidance and instructions for all NBS employees in case of a Departmentwide shutdown due to a lapse of appropriations. These instructions will be supplemented with notices and more detailed information immediately preceding the shutdown.

6.06.02

SCOPE

This subchapter applies to all NBS installations unless otherwise specified, i.e. NBS-Gaithersburg and NBS-Boulder.

6.06.03

POLICY

The shutdown of agencies of the Federal Government, due to a lapse in appropriations, is determined by the Antideficiency Act (July 1974) and by other applicable acts and rules governing Federal Civil Service. The applicable rules and acts have been interpreted by the Office of Management and Budget (OMB Bulletin No. 80-14, dated August 28, 1980) for general policy guidance in agency shutdowns. The Assistant Secretary of Administration, Department of Commerce, has provided policy guidance for Departmental shutdowns (memorandums of November 19, 1981, and December 7, 1981).

NBS is in a unique position in the Federal Government since it is authorized to use its Working Capital Fund (WCF) to accumulate various funds (see Section 6.06.06, Funding). In the absence of specific Departmental guidance, it is NBS policy to continue operation after a Departmental shutdown until the moneys available in the WCF are drawn down. Properly managed, the funds available in the WCF should allow near normal operation of NBS for some finite period of time.

6.06.04

DESIGNATION OF OFFICIALS

a. The following are the designated officials responsible for decisionmaking and reporting for NBS with regard to shutdown planning:

(1) Director, NBS-Gaithersburg;

(2) Associate Director for Programs, Budget, and Finance; and

(3) Director, NBS-Boulder
Laboratories - Boulder and field stations
(Ft. Collins, CO, and Kauai, HA).

b. The following are the designated shutdown coordinators:

November 20, 1987

(Trans. 601)

6.06.01 - 6.06.04

(1) Gaithersburg -

--Chief, Facilities Services Division to notify Bureau through the Cascade Alerting System and to maintain property integrity.

--Chief, Plant Division - to provide/maintain appropriate plant services.

--Chief, Personnel Division - to prepare written furlough/no furlough notices for issuance by supervisors.

(2) Boulder -

--Executive Officer - to develop/implement a site specific contingency plan to address the concerns of other agencies located on the Bureau's site.

6.06.05

RESPONSIBILITIES

a. The Associate Director for Programs, Budget, and Finance (ADPBF) shall be responsible for the following functions:

(1) Determining the amount of funds available in the WCF for reallocation to prevent immediate Bureau shutdown.

(2) Developing a contingency reallocation plan "to forestall the funding interruption date for the greatest number of employees for as long as possible."

(3) Recommending to the Director, NBS, minimum staffing levels, based on MOU information, for an extended shutdown after the WCF funds have been used up. (See Subchapter 6.06. Appendix A.)

(4) Serving as the point of contact for the Department to advise the Director, NBS, of developments and to channel related communications appropriately.

(5) Advising the Chiefs, Facilities Services Division, Plant Division, and Personnel of the decision to shutdown the Bureau in a timely fashion so that proper procedures are used.

(6) Coordinating overall notification of the Boulder site with the Director, NBS-Boulder Laboratories.

b. The Chief, Personnel Division, shall be responsible for preparing written furlough/no furlough notices for completion and issuance by an employee's immediate supervisor. (See Subchapter 6.06 Appendix B, Attachments 1, 2, & 3 for sample notices.)

c. The Chief, Facilities Services Division, shall be responsible for NBS-Gaithersburg shutdown procedures as per Subchapter 6.04, Facilities Self-Protection Plan.

d. The Facilities Services Division will provide to the Associate Director for Programs, Budget, and Finance a list of all individuals who enter and leave NBS during each day of the shutdown period. This report shall be submitted daily by 11:00 a.m.

e. The Executive Officer, NBS-Boulder, shall be responsible for developing a site specific contingency plan to address the concerns of other agencies located at that site. This plan shall be submitted through the NBS Emergency Planning Officer to the ADPBF.

6.06.06

FUNDING

a. NBS is authorized to accumulate funds into a Working Capital Fund from the following sources:

(1) Transferred funds from other agencies.

(2) Carryover funds from prior fiscal years that have been properly transferred and assigned for the current fiscal year.

(3) A leave fund approximately equivalent to the annual and sick leave accrued by NBS employees.

b. When a regular appropriation or a continuing resolution is not enacted by day X, the accumulated funds in the WCL may be made available to defray the cost of continued operations beyond day X until the WCF has been drawn down.

c. Forty to forty-five percent of the NBS daily operating cost is defrayed by other agency funds. Properly managed, the available STRS carryover and part of the OA funds will allow near normal operation of NBS for some period of time.

d. As soon as a Departmental shutdown has been declared, NBS will discontinue all procurement actions to preserve funding to meet the payroll. Exceptions must be expressly authorized by the Director of Administration. Purchases from the NBS Storerooms must be reduced to an absolute minimum.

e. In the event NBS must shutdown, a small staff will be employed to:

--protect Federal land, buildings, equipment, and other property owned by the U.S.; and

--maintain protection of research property.

All employees performing these excepted services are assured of the legal obligations of the Federal Government to make payment for these services, although the payments may be delayed.

6.06.07

DUTY STATUS OF EMPLOYEES

a. Assumes use of available appropriated and OA funds for up to six days. (Specific instructions on the number of funded work days available will be provided for each situation.)

(1) When a Department or Governmentwide shutdown is ordered, NBS will continue to work as usual with the exceptions listed in the next section. On the fourth day, travelers will be notified to conclude business and to return as soon as possible and no new travel will be started. If regular appropriations or a continuing resolution have not been enacted on the fifth day, NBS will use the sixth day of operation after funding lapse to prepare for a three-day shutdown (see below). Some equipment shutdown may have to start earlier to meet the maximum allowed staff levels.

(2) The NBS shutdown will begin on the specified day. If the situation persists, NBS will further reduce its maintenance effort on the tenth day to a continued shutdown level.

(3) All employees in duty status or on travel will be paid for work performed during the initial six days after the beginning of a Department shutdown.

(4) During the NBS three-day shutdown period, staffing will be reduced to the levels shown in Appendix A. These are maximum levels which cannot be exceeded without written permission from the Director or designee. The staffing levels shown are sufficient to protect buildings, equipment, and research property.

(5) For additional information concerning the Duty Station of Employees see Subchapter 6.06.07.b.(4)-(9).

b. Assumes immediate shutdown--available appropriation and OA funds not to be used.

(1) When a Department or Governmentwide shutdown is ordered, NBS will shutdown to the levels shown in Appendix A. If the shutdown lasts into the second day travelers will be notified to conclude business and return as soon as possible. No new travel will be authorized. If regulation appropriations or a continuing resolution have not been enacted on the second day, NBS will use the third day of operation after funding lapse to prepare for an extended shutdown (see below). Some equipment shutdown may have to start earlier to meet the maximum allowed staff levels.

(2) The NBS shutdown will begin on the first day. If the situation persists, NBS will further reduce its maintenance effort on the fourth day to a continued shutdown level.

(3) During the NBS three-day shutdown, staffing will be reduced to the levels shown in Appendix A. These are maximum levels which cannot be exceeded without written permission from the Director or designee. The staffing levels shown are sufficient to protect buildings, equipment, and research property.

(4) During the extended NBS shutdown, staffing levels will be further reduced.

(5) Employees not designated to be on duty by the Director, MOU Directors, Center Directors, or Division Chiefs (where appropriate) will be placed on annual leave. Employees who have exhausted their annual leave will automatically be furloughed.

(6) Under no circumstances may an employee be granted unaccrued leave to be taken during the NBS shutdown.

(7) Employees who are on sick leave at the beginning of the NBS shutdown may remain on sick leave until they recover or exhaust accrued sick leave. They may then transfer to annual leave, if available, or will be furloughed. Sick leave may be granted to employees who are on annual leave but not to employees who are furloughed.

(8) The end of the shutdown will be announced as part of the general news by local papers, radio, and television. There will be an appropriate tape message on the Bureau's general telephone number, 975-2000.

6.06.08

NBS SHUTDOWN OPERATIONS

a. Technical Centers and Divisions

(1) During the first three days of NBS shutdown, Center Directors or Division Chiefs (where appropriate), or appropriate persons designated by these officials (or Office Chiefs), will work with designated technical support staff on necessary maintenance functions such as maintaining high vacua, cryogenic or other critical temperatures, checking operation of computers, etc. The staff levels authorized for these functions are listed in Appendix A. Actual staffing should stay below these levels. The listed levels cannot be exceeded without the express permission of the Director or designee.

(2) At the time of a shutdown, timekeepers should complete time and attendance worksheets up to that point, and deliver them to their Center or Division (where appropriate) Offices (Financial Information Office in Boulder), where they will be held until resumption of Bureau operations or entered into the payroll system if Bureau operations do not resume before the end of the pay period.

(3) During an extended shutdown, the staffing levels are further reduced. All maintenance functions will be performed by appropriate technical support staff.

(4) Particular attention must be paid to the observation of all safety rules and precautions. If the shutdown extends beyond three days, it is very possible that operating equipment will receive less attention than is normal and, therefore, the risk of an emergency situation occurring is much greater. The Fire Protection Service (Physical Security in Boulder) should be notified of the location of any equipment, other than Plant equipment, that will be left operational during the shutdown period. This information will allow our fire and security personnel to check on the few people who will be working, perhaps alone, in a laboratory environment and subject to a greater safety problem than during periods of normal operation.

(5) There is no authority to accept voluntary services of NBS employees during a shutdown. The Attorney General's opinion makes it clear that accepting voluntary services would be in violation of the Antideficiency Act. Employees not designated for the performance of minimum maintenance services will, therefore, not be permitted on the NBS sites.

(6) By noon of the second day following the shutdown, MOU Directors shall submit to the Associate Director for Programs, Budget, and Finance their further reduced staffing level for an extended shutdown (beyond three days). Staffing for the extended shutdown may not exceed 70% of the level approved for the first three (3) days.

b. Administrative and Technical Support Divisions

(1) The Offices of the NBS Director, and the Offices of the Directors of NML, NEL, ICST, IMSE, and ADMIN will be staffed to provide the necessary minimum of supervision and coordination. Also follow IV.A.2.

(2) The Plant, Facilities, Acquisition and Assistance, and Personnel Divisions and the Comptroller's Office will be staffed to provide minimum services. In case of severe snow fall, the Ground Crew will keep fire lanes open and, before reopening the site after NBS shutdown, will open access to the site. Both Plant Divisions are authorized to call back craftsmen to make emergency repairs.

(3) Since the support divisions services during a shutdown will not change sufficiently over time, staffing levels for a three (3) day and extended shutdown have already been established.

c. Services to be Maintained

(1) Utilities: electricity, gas, water, steam, chilled water, and compressed air will be available as usual.

(2) Cryogenic liquids and dry ice will be delivered to laboratories and/or the usual pick-up points; schedule must be arranged before the shutdown of NBS.

(3) Heat and air conditioning will be on night and weekend service.

(4) If payday occurs while NBS is shutdown, payroll for work performed before NBS shutdown will be processed. Employees whose bank accounts are normally credited with their paycheck or have their checks mailed home will receive these funds as usual. Employees who normally receive their paycheck on-site see page 1, Abstract #1.

(5) Signet Bank and Credit Union will be open on Thursday, the normal payday.

(6) Incoming mail will be sorted but not delivered.


(7) The NBS telephone number, 975-2000, will be answered by a tape announcing the shutdown and directing all urgent calls to the Director of Administration, 975-2390. The staff in the Office of the Director of Administration will then direct these calls to the appropriate staff, if available.

NOTE: Only work directly connected with the shutdown, with the protection of Government property, and the safety of staff may be carried out. Supervisors are responsible for the observation of this rule. ■■■■

APPENDIX A

MAXIMUM STAFF LEVELS DURING NBS SHUTDOWN

The attached Maximum Staff Levels Chart (Attachment 1) lists the staff necessary to provide a minimum of oversight, budget, accounting, and personnel functions, maintenance of plant and facilities, and maintenance of experimental equipment that cannot be shut down. NBS will provide low level guard and fire protection service, air conditioning, gas, water, chilled water, electricity, and liquid nitrogen and dry ice at the usual points of service. Each Center Director or Division Chief (where appropriate) will decide which equipment must and can be maintained in operation during a shutdown. During a short (three day) shutdown or during the first three days of a long shutdown, these officials, or suitable persons designated by them, will coordinate the work of technicians maintaining operating and nonoperating equipment. This may include replenishing liquid nitrogen or dry ice, warming equipment up to room temperature, etc. For long shutdowns, the technicians will continue to carry out the maintenance work. Other staff will assist only if urgently needed and only with express permission of the Center Director/Division Chief or Deputy.

The staff levels listed show the maximum number of staff authorized to work on the NBS sites during a shutdown but do not include the staff needed to distribute paychecks if a payday falls into the shutdown period. Supervisors are responsible to the Director for accomplishing all tasks at the smallest expense compatible with prudent management and safe operation. 

APPENDIX A - ATTACHMENT 1

MAXIMUM STAFF LEVELS

<u>Division</u>		<u>3 Days</u>
100	<u>NBS Director's Office/OADPF</u>	
	Director, Deputy, Secretary	3
104	<u>Director, NBS Boulder Laboratories</u>	
	Director, Secretary	2 5
110	<u>Office of the Associate Director for Programs, Budget, and Finance</u>	
	Associate Director, Secretary	2
111	<u>Program Office</u>	
	Analyst	1
112	<u>Budget Office</u>	
	Supervisor (1) Senior Analysts (2) Analysts (2)	5
113	<u>Comptroller's Office</u>	
	Comptroller or Deputy (1) Secretary (1) Supervisor (1) OA Contracts (1) Accounts Payable (1) Accounts Receivable (2) Document Control, Acct. Rep. (3) Accounting (2)	12 20
130	<u>Office of the Associate Director for Industry and Standards</u>	0
320	<u>Director of Administration</u>	
	Director or Deputy (1) Secretary (1)	2
351	<u>Plant Division</u>	
	Supervisor (1) Secretary (1) Steam Plant, 3 shifts (14) AC maintenance (4) Grounds Crew (23), when needed	43 70

353	<u>Facilities Services Division</u>	
	Supervisor (1)	
	Secretary (1)	
	Guards, 3 shifts (15)	
	Firemen, 3 shifts (12)	
	Janitors (2)	
	Mailroom (2)	33
354	<u>Health and Safety</u>	
	Health Physicist on call	
355	<u>Personnel Division</u>	
	Personnel Officer or designated rep. (1)	
	Processing Supervisor (1)	
	Team Leader (3)	
	Generalist (4)	
	Personnel Clerk (4)	
	Payroll (2)	13
357	<u>Acquisition and Assistance</u>	
	Storeroom (IN and CO ₂ distribution) (2)	2
		118
360/363	<u>Boulder Executive Office and Plant Division</u>	
	Supervisors (2)	
	Secretaries (2)	
	Mechanical (3)	
	Electrical (1)	
	Buildings (1)	
	Grounds (7)	
	Custodial (2)	
	Guards, 3 shifts (14)	32
400	<u>Institute for Materials Science and Engineering</u>	15
500	<u>National Measurement Laboratory</u>	34
600	<u>Institute for Computer Sciences and Technology</u>	2
700	<u>National Engineering Laboratory</u>	19
		220

APPENDIX B

SOME EFFECTS OF FURLOUGH STATUS

1. Furlough time up to 30 days counts toward completion of probationary period and completion of career tenure requirements.
2. SES employees, temporary employees, employees serving probationary periods, excepted service non-preference eligibles with less than one year of current continuous service and others not covered by Part 752 of the Civil Service Regulations are not entitled to appeal rights as described for other employees.
3. Employees continue to earn annual and sick leave, but on a pro rata basis, for partial pay periods on furlough. No leave is earned for a full pay period on furlough.
4. Sick leave may not be substituted for furlough time.
5. Retirement, life insurance and health benefits coverage continue during short furloughs, without charge to the employee. If retroactive appropriations cover the furlough and the employee is paid salary for the furlough time, regular deductions are withheld from the retroactive payment.
6. Attachments 1, 2, and 3 provide samples of letters to employees for furlough/non-furlough conditions.

APPENDIX B - ATTACHMENT 1

SAMPLE LETTER FURLOUGH

(For all employees whose positions are not essential to protection of life and property, other authorized activities, or the orderly suspension of operations.)

Dear _____

At midnight, _____ (the Continuing Resolution) expired. The Department of Commerce now has no annual appropriation and must suspend most non-essential operations until new appropriations are available.

The services of your position are not essential to the protection of life and property, to activities otherwise authorized by law, nor to an orderly suspension of operations. It is necessary, therefore, to place you on annual leave until your accrued annual leave is exhausted at which time you will be placed on furlough, without pay, for a period not to exceed 30 calendar days. Since this furlough is caused by an emergency situation arising out of circumstances beyond the control of the Department, we regret that it is impossible to give you a longer notice period.

As soon as this furlough is ended, we will promptly make every attempt to inform you and other furloughed employees through a news release to local radio, TV, newspapers, by telephone, or by the U.S. mail. Please keep a close monitor on all local news media for this information, which will instruct you when to return to your job.

Except for SES appointees for whom there is no appeal right, employees in the competitive civil service who have completed at least one year of current continuous employment under a non-temporary appointment may appeal this action to the Merit Systems Protection Board (MSPB). Preference eligibles in the excepted service who have completed at least one year of current continuous service in the same or similar positions may also appeal to the MSPB. Employees with MSPB appeal rights who are covered by a negotiated grievance procedure may file a grievance under that procedure. Employees with neither MSPB appeal rights nor access to negotiated grievance procedures may file a grievance under the grievance procedures of their organization.

The attached information explains the effect of furlough on leave, retirement, insurance, and other benefits. Your personnel office will be able to handle any general questions you may have.

We regret this inconvenience to you.

Sincerely,

(Supervisor)

Attachment

APPENDIX B. - ATTACHMENT 2

SAMPLE LETTER - NO FURLOUGH - I

(For employees whose position is essential to enable orderly suspension of operations.)

Dear _____

At midnight on _____ (the Continuing Resolution) expired. The Department of Commerce now has no annual appropriation and must suspend non-essential operations until new appropriations are available.

Your position is essential to enable an orderly suspension of operations. You are, therefore, requested to continue working temporarily in your essential position for the sole purpose of assisting in an orderly shutdown of operations.

During this period funds may not be available for the payment of salaries, but we assure you that the Department of Commerce will not contest its legal obligations to make payment to you for these services.

Your personnel office will be able to handle any questions you may have.

Sincerely,

(Supervisor)

APPENDIX B - ATTACHMENT 3

SAMPLE LETTER - NO FURLOUGH - II

(For employees asked to stay on to continue in positions essential to protection of life and property or essential to activities otherwise authorized by law (such as national security, foreign relations necessary to national security, providing benefit payments, contract obligations under no-year or multi-year funds still available.)

Dear _____

At midnight on _____ (the Continuing Resolution) expired. The Department of Commerce now has no annual appropriation and must suspend most non-essential operations until new appropriations are available.

Your position is essential to enable the continuance of activities otherwise authorized by law, or to protect life and property. You are, therefore, requested to continue working in your essential position indefinitely.

During this period funds may not be available for the payment of salaries, but we assure you that the Department of Commerce will not contest its legal obligation to make payment to you for these services.

Your personnel office will be able to handle any questions you may have.

Sincerely,

(Supervisor)

6.07 Building 101 Corridor Utilization Policy

6.07.01

PURPOSE

This chapter establishes policy for the safe use of corridors for displays and tables within the Building 101 conference facility area at the NIST Gaithersburg location.

6.07.02

SCOPE

This subchapter applies to all NIST employees and visitors who use the corridors in the Building 101 conference facility area for conference activities and displays.

6.07.03

POLICY

It is the policy of DoC and NIST to provide an effective fire prevention and protection program to reduce loss of life and property from fire and also provide high quality emergency medical care. All displays and exhibits in the described area must be set up and maintained in accordance with NFPA 101 Life Safety Code and 29CFR1910 and directions provided by the NIST Fire Protection Group (FPG) and NIST Safety Office (NSO).

6.07.04

AUTHORITIES

29 CFR 1910 Subpart E, Means of Egress

NFPA 101 Chapter 7, Means of Egress and Chapter 10, Interior Finish, Contents, and Furnishings, 2006 Edition

6.07.05

RESPONSIBILITIES

- a. Conference Facility staff and Public and Business Affairs and other Sponsors are responsible for ensuring that all events using corridors are conducted in a manner that maintains an adequate means of egress in the event of a fire or other emergencies.
- b. The Division Chief and group leaders are responsible for ensuring that this policy on means of egress is followed.
- c. At NIST Gaithersburg the FPG and NSO are responsible for providing additional guidance or interpretation of the provisions of this policy; conducting periodic inspections of NIST corridors for the purpose of advising corridor users of

conditions requiring corrective action and taking immediate action to bring about the removal of items that would prevent safe egress of building occupants.

6.07.06

CORRIDOR USE PROCEDURES

- a. A minimum of 72 inches' width of clear and unobstructed egress shall be maintained at all time in the South Corridor by the Green Auditorium and in the East Corridor by Lecture Rooms A and B. Any display tables or posters shall be kept to one side of the corridor at all times. Posters should be hung on poster board to the rear of the tables and on the designated poster display boards across from the Red Auditorium.
- b. The West Corridor, by Lecture Rooms C and D shall be kept free and clear of all obstructions. Unobstructed egress shall be maintained at all times.
- c. A display area by the bank of elevators shall be permitted on a limited basis. Tables may be placed beside the elevators on the south wall facing the permanent NIST exhibits. No tables will be placed in the immediate vicinity of elevator doors. All displays shall be constructed of non-combustible materials. A minimum of 36 inches' isle width must be maintained as a walking space at all times.
- d. Lobby displays are permitted on a limited basis. A single table may be placed by the column near the reception desk. This guidance applies to the location for the annual holiday celebration tree and CFC display. In addition to the table, one easel may be placed in front of the column. These easels may be placed under the LED screen display in the Lobby adjacent to the reception desk along the marble wall. At no time will the displays impede the means of egress from the Building 101 Lobby from any direction.

6.07.07

APPROVAL

No less than forty-eight hours prior to the event the event Sponsor will work with Conference Facilities to coordinate pre approval of plans and set up with Public and Business Affairs, NIST Fire Protection Group and the Safety Office. All displays shall be removed within 48 hours after the end of the event.

Appendix A:

Selected Extracts from 29 CFR

Maintenance, safeguards, and operational features for exit routes. - 1910.37

1910.37(a)

The danger to employees must be minimized.

1910.37(a)(1)

Exit routes must be kept free of explosive or highly flammable furnishings or other decorations.

1910.37(a)(3)

Exit routes must be free and unobstructed. No materials or equipment may be placed, either permanently or temporarily, within the exit route. The exit access must not go through a room that can be locked, such as a bathroom, to reach an exit or exit discharge, nor may it lead into a dead-end corridor. Stairs or a ramp must be provided where the exit route is not substantially level.

1910.37(b)(3)

Each exit route door must be free of decorations or signs that obscure the visibility of the exit route door.

1910.37(b)(4)

If the direction of travel to the exit or exit discharge is not immediately apparent, signs must be posted along the exit access indicating the direction of travel to the nearest exit and exit discharge. Additionally, the line-of-sight to an exit sign must clearly be visible at all times.

Administrative Manual Section 7.02 Maintenance, Modifications, Improvements, and Replacement - Facilities Management

Sections

- 7.02.01 Purpose
- 7.02.02 Scope
- 7.02.03 References
- 7.02.04 Policy
- 7.02.05 Definitions
- 7.02.06 Authority and Limitations
- 7.02.07 Responsibilities for Facilities Management
- 7.02.08 Financing
- 7.02.09 Charges for Plant Services
- 7.02.10 Radio Transmitter Installation
- 7.02.11 Antennas and Similar Equipment
- 7.02.12 Building Exteriors, Paved Areas, and Lawns
- 7.02.13 Public Areas, Corridors, and Lobbies
- 7.02.14 Air-Conditioning Equipment
- 7.02.15 Conservation of Resources
- 7.02.16 Planned Utility Service Interruptions (Gaithersburg)
- Appendix A - Requesting Maintenance, Modifications, Improvements, and Replacements
- Appendix B - Financing and Control of Laboratory Furniture and Metal Partitions
- Appendix C - Maintenance of Refrigeration and Air-Conditioning Equipment

7.02.01 PURPOSE

This subchapter prescribes NIST policy and procedures for maintenance, modifications, improvements, and replacement of facilities.

7.02.02 SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

7.02.03 REFERENCES

Administrative Manual Subchapter 7.03, Leasing Real Property
Administrative Manual Subchapter 7.08, Space Management
DAO 216-6, Implementing the National Environmental Policy Act
DAO 217-1, Real Property Management Manual, Introduction
DAO 217-16, Energy Conservation
OMB Circular A-104, Evaluating leases of capital assets (tangible property: of \$1 million +, including durable goods, equipment, buildings, facilities, installations or land).
15 U.S.C. 278 c. Acquisition of land for field sites, d. Construction and improvement of buildings and facilities (NIST), e. Functions and activities (NIST)

40 U.S.C. 14a Construction, alterations, improvements ... buildings, grounds, facilities

40 U.S.C. 490(d)(5) Operation of bldgs. ... transfer of functions

7.02.04 POLICY

a. NIST is authorized under specific conditions (40 U.S.C. 14a) to undertake the construction of buildings and other facilities, to make alterations and improvements to existing buildings, grounds, and other facilities it occupies or uses, to care for, maintain, and protect the buildings occupied, and to replace aging and deteriorating facilities to promote the proper and efficient conduct of its activities.

b. Acquisition of real property and replacement of facilities are made only when such actions can be adequately justified to the Director for Administration and Chief Financial Officer (DA/CFO) as being essential for the conduct of new or expanded programs or for increased efficiency or economy of operations and funds are approved by the Budget Division.

c. Construction projects which could significantly affect the quality of the human environment may require an environmental impact statement. Prior clearance and approval of the National Capital Planning Commission is required for proposed projects at Gaithersburg which would change materially the outward appearance of buildings, roads, or landscape.

d. The building of temporary structures and antennas on NIST grounds (Gaithersburg) also requires approval by the National Capital Planning Commission. The DA/CFO considers requests for the approval of temporary structures after evaluation by the Plant Division in accordance with the following criteria:

(1) A thorough examination of all alternatives reveals that no other alternatives are available;

(2) The proposed structure will not have a negative effect on the local surroundings either aesthetically or environmentally;

(3) The facility will be required for a specified period of time after which it will be dismantled and the area restored to its original state; and

(4) All work such as construction, maintenance, dismantling, and restoration of the area will be funded by the sponsoring division.

e. Facilities improvements, modifications, and replacement of aging facilities must be approved by the Plant Division/Engineering, Maintenance, Safety, and Support Division regardless of the source of funds. Appeals may be made to the Deputy Director for Safety and Facilities, Gaithersburg or the Director, NIST/Boulder Laboratories.

f. Equipment needed for the operation of a new facility to be financed under the Scientific and Technical Research and Services (STRS)/Construction Research Facilities (CRF) Programs may be requested along with the facility construction or acquisition funds in connection with the annual budget requests. Individual items of equipment costing over \$350,000 may also be

requested under the STRS/CRF Programs. Requests for permanently installed equipment items costing under \$350,000 each may be considered in special cases involving several like items required for a single program.

g. Increases in staff or operating costs resulting from approved improvement and modification projects are the responsibility of the requesting organizational unit. These increases must be absorbed even though the requesting memorandum outlines the need for additional staff or operating funds.

h. Replacement of aging plant and facility equipment is initiated by the Plant Division/Engineering, Maintenance, Safety, and Support Division and approved by the Deputy Director for Safety and Facilities. Planned systematic replacement of aging plant and facility equipment is based on engineering, economic, and operations research data. The data is derived from:

(1) Interviews with engineering and operating employees of the Plant Division/Engineering, Maintenance, Safety, and Support Division;

(2) Previous NIST budgets for facility maintenance, modifications, and improvements;

(3) On-site inspections of both physical plants;

(4) Equipment service life data from the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE); and

(5) Cost data from local area governments, manufacturers, contractors, and the most recent edition of the R.S. Means Mechanical and Electrical Cost Data Guide.

7.02.05 DEFINITIONS

a. Maintenance is the upkeep of plant facilities to ensure a condition of efficiency and utility, including predictive maintenance, scheduled periodic preventive maintenance, routine maintenance and repair (usually unscheduled and of a minor nature reflecting fair-wear-and-tear), and major repair and replacement caused by failure or predicted failure of major facilities systems or components. Preventive maintenance and routine maintenance and repair are funded by Institute overhead. Major repair and replacement may be funded by Institute overhead or by the annual STRS/CRF appropriations to the extent that such appropriations are available.

b. Modification is the rearrangement or preparation of existing space or facilities to make them more useful for conducting NIST work. This includes modifications which enhance the working conditions and effective use of existing NIST space and facilities without adding thereto. Modification costs are not capitalized. Extensive modifications may require specific written explanation to the sponsoring OU Director as to why the work should not be considered an improvement.

c. Improvement is a valuable and useful permanent addition to building space or facilities such as permanent air-conditioning systems, sidewalks, roads, fences, etc. Separate cost centers are established in each case to accumulate costs for capitalization purposes. Improvements do not include temporary special purpose structures which are shelters for or part of equipment for experiments; repairs to roofs and roadways; or repairs and replacement of utilities.

d. Systematic replacement is the replacement of obsolete or aging equipment that is predicted to fail and becomes unserviceable or uneconomical to repair. Replacement avoids emergency repair work and costly downtime while major repairs are made. Predictions are based on the equipment service life and other factors mentioned in Section 7.02.04. The decision to replace aging and deteriorating equipment is influenced by the following factors:

- (1) Replacement with an identical item becomes less costly than continued maintenance and repair;
- (2) Replacement with an identical item becomes necessary to ensure reliability or safety;
- (3) Advanced technology suggests replacement due to lower operating costs for new equipment;
- (4) Changing requirements necessitate replacement to meet new needs not within the capabilities of existing equipment; and
- (5) Energy conservation measures dictate replacement to reduce energy consumption.

e. Facilities include buildings, roads, grounds, sidewalks, fences, equipment, and underground utility distribution systems.

f. Project-related (or task-related) refers to maintenance, modifications, or improvements which are essential to the performance of a particular project (task) within a division. In the case of maintenance, project-related maintenance is that which is required beyond the general level scheduled for NIST. An example of such maintenance would be the replacement of resins in a water purification system associated with a technical project. Improvements or modifications in this category are changes or additions required solely for the particular activity involved and would be unnecessary for other building occupants. The fact that space is assigned to a project (or task) is considered evidence that the proposed modification or improvement is project-related.

7.02.06 AUTHORITY AND LIMITATIONS

a. Funds appropriated to NIST are available for:

- (1) The construction of buildings and other facilities, maintenance, modification, and improvements to existing buildings, grounds, and other facilities occupied or used by NIST in Gaithersburg and Boulder, and the replacement of facilities at the NIST-Gaithersburg and NIST-Boulder sites, as are necessary for the proper and efficient conduct of its activities.

(2) The maintenance and modification of buildings and other plant facilities at rented field sites, laboratory, office, and warehouse space outside the Washington Metropolitan Area (15 U.S.C. 278e).

(3) The building of specialized facilities and working and living quarters on leased property when serving the interests of the government (15 U.S.C. 278e). General, large-scale improvements on leased property are not contemplated under this authority. This authority is used only if supported by the expected length of occupancy of the site and the nature of the facilities to be constructed. Ordinarily, the facilities are of a special nature and do not enhance the value of the property to the owner.

b. Funds received from other federal agencies are available for improvements only when either expressed or implied authority is found in the act appropriating the funds. NIST is subject to the same Congressional limitations as are imposed on the transferring agency. The Budget Division must verify fund availability for improvements. Other-agency funds are available for project-related maintenance and modifications unless specifically prohibited by the terms of the order.

c. Alterations and improvements to leased property are subject to the following restrictions and conditions:

(1) Expenditures for alteration, improvements, and repairs to rented premises may not exceed 25 percent of the annual rent for the first year of the term or 25 percent of the rental if the rental term is less than one year. However, the installation of special facilities which are essential to carry out the program assigned to leased premises are not considered to be subject to the limitation if the facilities do not contribute to the general use and purpose of the building, and title, and right to remove them is reserved to the government.

(2) The 25 percent limitation does not apply to unimproved land leased as such.

d. Congressional approval must be obtained prior to the purchase of land.

7.02.07 RESPONSIBILITIES FOR FACILITIES MANAGEMENT

a. The Deputy Director for Safety and Facilities initiates and reviews requests for major modifications, improvements, and replacements of facilities to assure the most effective use of present and new facilities, to coordinate current and long range planning for new facilities with NIST technical program objectives and to ensure compliance with congressional statutory limits. The DA/CFO gives final approval of requests and forwards a list of planned projects to the Budget Division for approval.

b. The Budget Division reviews requests for modifications, improvements, and replacements, works with the DA/CFO and the Chiefs of the Plant Division and Engineering, Maintenance, Safety, and Support Division to further develop the plan for spending the CRF allocation, and makes recommendations to the DA/CFO on the availability of funds. Approval of the plan must be given by the Budget Division before any funds are released.

c. The Plant Division/Engineering, Maintenance, Safety, and Support Division are responsible for the design, construction, and maintenance of -the Physical Plant- all buildings, building equipment, structures, roads, grounds, and utility systems for NIST-Gaithersburg, NIST-Boulder, and Fort Collins, Hawaii Field Sites, respectively. They are the only divisions authorized to modify the NIST Physical Plant. They are also responsible for the following functions relating to the operation, maintenance, modification, improvement, and replacement of NIST facilities:

(1) Review plans for proposed improvement, modification, or replacement of buildings, grounds, and facilities to be done either by NIST employees or by contract to determine propriety and compliance with site development plans. Prepare or have prepared an environmental impact statement if required.

(2) Supervise or perform all maintenance, modifications, improvements, and replacements within authorized funds.

(3) Coordinate negotiations on behalf of NIST staff with architects, construction contractors, and other agencies.

(4) Approve requests for the installation of environmental air-conditioning and refrigeration equipment and their maintenance.

(5) Notify the Office of the Deputy Director for Financial Services and Deputy CFO of the completion of improvements so they may be capitalized.

(6) Request clearance and approval of projects with the National Capital Planning Commission (Gaithersburg). See Section 7.02.04.

7.02.08 FINANCING

a. The appropriate source of financing for maintenance, modifications, improvements, and replacements depends upon the nature of the work. Improvements may not be charged to Institute or OU overhead without prior approval from the Budget Division. (See Section 7.02.05 for definitions of terms.)

b. Costs are charged to the following sources of financing:

(1) Routine maintenance and repairs: Institute overhead.

(2) Other maintenance and modification: Benefiting cost center, Institute overhead, or CRF, as appropriate.

(3) Improvements, major repairs, replacements, and permanently installed major equipment over \$350,000: STRS and CRF appropriations. A separate cost center shall be established for each improvement to accumulate costs for capitalization. Financing is assigned from the benefiting cost center.

Note: Unobligated balances of STRS and CRF allocations for line items and miscellaneous projects are withdrawn on completion of the project. See Subchapter 8.04.

7.02.09 CHARGES FOR PLANT SERVICES

- a. Estimates for Plant services requested on Form NIST-461, Interdivision Work Order, are provided by a Plant Division/Engineering, Maintenance, Safety, and Support Division engineer or technician based on the work described and in consultation with the originator.
- b. Engineering design and estimating time are included in the cost of the work, except on those requests in which the total cost of construction is less than \$2,000. However, if the scope of work is increased beyond \$2,000 after the initial estimate, all design/estimating charges are charged to the requesting cost center. On projects with an estimated cost of \$2,000 or more, the design/estimating costs are charged to the requesting cost center, even though the order may be canceled upon receipt of the estimate from the Plant Division/Engineering, Maintenance, Safety, and Support Division.

The Plant Division/Engineering, Maintenance, Safety, and Support Division provides minor consulting services and prepares project estimates for projects under budget proposal for the STRS and CRF Programs at no cost to the requesting division. However, if the request requires extensive work and the workload becomes excessive, the Chief of the Plant Division contacts the Director for Administration and Chief Financial Officer to determine the source of payment.

- c. Funds available in one year cannot be legally obligated for Plant Division/Engineering, Maintenance, Safety, and Support Division services to be performed in the following year except for STRS and CRF funds. Prices for jobs not completed during the fiscal year are adjusted at the end of the fiscal year to reflect the estimated cost of that portion of the work which is completed. The balance of the work to be completed is reobligated in October against funds available in the new fiscal year. This should be kept in mind when planning jobs to be charged to projects financed from one-year funds to ensure that sufficient funds are available in the subsequent year(s) to cover the job until completed.
- d. The estimated cost for each Form NIST-461, Interdivision Work Order, as determined by the Plant Division/Engineering, Maintenance, Safety, and Support Division, is the fixed price for the work. This amount is charged to the benefiting cost center prior to initiation of the job. The fixed price is revised when changes are requested by the originating division. The Plant Division/Engineering, Maintenance, Safety, and Support Division may charge actual costs for jobs of extended duration, "short-form" jobs (time and materials), or for jobs that do not lend themselves to a fixed-price estimate. The requester is informed in advance in such cases. "Fast-Track" jobs are done on a design-as-you-go basis with charges not to exceed 25 percent of the authorized rough estimate.

7.02.10 RADIO TRANSMITTER INSTALLATION

- a. Gaithersburg - Approval of the Director for Administration and Chief Financial Officer must be obtained before any radio transmitting equipment is installed in or on any building at NIST-

Gaithersburg. Requests should clearly describe the type of transmitter to be installed, including the voltage, wattage output, frequency, and antenna required.

b. Boulder - A memorandum must be submitted to the Interference Committee through the Engineering, Maintenance, Safety, and Support Division, NIST/Boulder Laboratories by anyone planning to install a transmitter or other equipment or to perform tests likely to emit electromagnetic waves that might cause interference. The memorandum should describe the equipment or tests in sufficient detail for the Committee to determine the probable interference with other work.

7.02.11 ANTENNAS AND SIMILAR EQUIPMENT

a. The roofs of the Gaithersburg buildings are not designed or constructed to accommodate equipment or recurring personnel traffic. Therefore, no experiments can be conducted or equipment mounted on the roofs. Antennas for radio, television, and/or other sensing devices (wind, temperature, barometer, etc.), are approved only if they are an integral part of a NIST program and vital to the NIST mission, as determined by the Director for Administration and Chief Financial Officer.

b. Requests for exceptions to and/or approval of the above should be submitted by memorandum through the respective OU office to the Director for Administration and Chief Financial Officer. Requests should include the anticipated duration of the requirement, the proposed location, and a statement of need. Preliminary consultation with Plant Division is encouraged. If the duration of the requirement exceeds the duration of a previously approved request, a rejustification and submission by the project sponsor with specific concurrence of the OU Director is required.

c. If it is determined that an antenna or an equipment installation is vital and is approved, the Plant Division works with the sponsoring division to determine the best possible means of installation at the least objectionable location.

d. The Plant Division, at the direction of the Director for Administration and Chief Financial Officer, requests clearance and approval of projects with the National Capital Planning Commission (Gaithersburg).

e. Boulder - Requests for roof-placed equipment requires location approval by the Chief, Engineering, Maintenance, Safety, and Support Division.

7.02.12 BUILDING EXTERIORS, PAVED AREAS, AND LAWNS

a. For ease of maintenance and aesthetics, the following restrictions apply: (1) no attachments to building exteriors are permitted; (2) equipment installations and testing on lawn areas are prohibited except for periods of specified and short duration; and (3) mobile homes, storage trailers or containers, or similar mobile equipment or transportable apparatus must not be sited on lawn or paved areas without prior approval of the Director for Administration and Chief Financial Officer.

b. Requests for exceptions to and/or approval of the above must be submitted through the respective OU office to the Director for Administration and Chief Financial Officer, as described in Section 7.02.11.

c. An area on the south end of the Gaithersburg site has been designed for long-term outdoor exposure testing. Requests for using this site must be submitted to the Director for Administration.

7.02.13 PUBLIC AREAS, CORRIDORS, AND LOBBIES

Public areas are the responsibility of the Director for Administration and Chief Financial Officer and are not to be used for experimental purposes due to potential safety hazards. Similarly, corridors are to be kept clear of bulky equipment, furniture, files, etc., and are not to be used to meet storage, laboratory, or office space requirements. Temporary exceptions may be granted during space modifications.

7.02.14 AIR-CONDITIONING EQUIPMENT

a. Portable air-conditioning is equipment that can be installed and removed without appreciably damaging or defacing the equipment or the premises. It may serve several rooms, may be moved from one location and satisfactorily installed in another, may require ducts for the distribution or return of air, or may require plumbing. These are to be considered as equipment and may be procured from equipment funds as outlined in Subchapter 8.11.

b. Permanent air-conditioning is equipment that is attached to the premises and is considered part of the realty. The following must be considered permanent air-conditioning equipment: (1) air-conditioning equipment involving ducts and/or plumbing which is built into the walls, partitions, or ceilings of a structure, and (2) air-conditioning equipment which is designed and built for a specific location and which would not be suitable in another location. Permanent air-conditioning equipment is classified as an improvement and may be procured only with funds appropriated to NIST with specific legal authorization to be used for this purpose. Approval procedures for improvements outlined in this subchapter are to be followed.

c. Requests for purchase and installation of air-conditioning equipment must be submitted on Form NIST-461, Interdivision Work Order, and forwarded to the Plant Division/Engineering, Maintenance, Safety, and Support Division for review and approval.

7.02.15 CONSERVATION OF RESOURCES

a. Fuel - The heating and cooling of the buildings is thermostatically controlled in accordance with established design criteria. The thermostats are set by authorized employees of the Plant Division to provide a balanced comfort condition. Room thermostats are not to be adjusted or tampered with by employees. Notify the Plant Division/Engineering, Maintenance, Safety, and Support Division when adjustments are necessary.

b. Water - To conserve water, the circulating chilled water system must be used for equipment cooling wherever possible. Approval is not given for installation of equipment which uses over two gallons per minute of uncirculated water. All equipment using uncirculated water must be turned off when not in actual use. Leaking pipes, faucets, or other fixtures should be reported promptly to the Plant Division. If reported leaks are not repaired within seven calendar days, the problem should be reported in writing to the Director for Administration and Chief Financial Officer.

c. Measures employees can take to conserve resources:

(1) Turn off all machinery, including office equipment, when not in use;

(2) Turn off lights when leaving a room for 15 minutes or more;

(3) Leave corridor lights at their reduced level;

(4) Use natural daylight in exterior rooms, including restrooms;

(5) Do not use unauthorized electric heating appliances;

(6) Do not cover the top or the front of window induction units; this restricts air flow and reduces heating or cooling capacity;

(7) Close blinds to screen the sun during hot weather. During cold weather, close blinds overnight but keep open during daylight hours to capture the sun's heat. Procedures should be opposite for heat-generating areas on year-round air-conditioning (example: computer facility); and

(8) Do not adjust heating/air-conditioning room thermostats.

7.02.16 PLANNED UTILITY SERVICE INTERRUPTIONS (GAITHERSBURG)

a. The Plant Division may authorize interruptions of utility services to meet emergency conditions or where scheduled maintenance or construction can be accomplished by no other means. Every precaution is taken to ensure minimum interference with technical projects. Full use is made of each scheduled outage to permit coordinated simultaneous performance of associated maintenance work.

b. The Operations Engineering Group is responsible for scheduling and coordinating all planned interruptions of utility services and for liaison with groups affected by or requesting such outages. The Operations Engineering Group maintains a current list of key division personnel in various buildings to be notified whenever interruptions occur under emergency conditions, or when outages are planned for routine purposes. During extraordinary situations the Cascade system may be used; see Subchapters 6.02, 6.03, and 6.04 for details.

c. It is the responsibility of key division personnel to notify all employees designated by their supervisor that may be affected by an upcoming Utility Service Interruption. The Operations Engineering Group must be notified when key division personnel change.

d. When the Operations Engineering Group determines that a planned outage is sufficiently widespread, Form NIST-398, Notice of Outage Sitewide, is distributed by mail throughout NIST. This notice provides details of the outage, including date, period of time, and buildings or systems affected. The Notice of Outage Sitewide is distributed no less than a week in advance of the planned outage to permit technical divisions to schedule (reschedule) programs and request temporary service if necessary.

BUILDING DESIGNATIONS

Sections

7.04.01 Purpose

7.04.02 Scope

7.04.03 Policy

7.04.04 Procedures

7.04.01

PURPOSE

The purpose of this subchapter is to establish a standard procedure for the numbering and naming of buildings at NIST.

7.04.02

SCOPE

This subchapter applies to the numbering and naming of buildings at both the NIST-Gaithersburg and NIST-Boulder sites.

7.04.03

POLICY

It is NIST policy that all buildings at the Gaithersburg and Boulder sites be numbered and named. Changes in building designations, either the name or the abbreviation, are prohibited except as outlined in this subchapter.

7.04.04

PROCEDURES

a. **Numbering Buildings** - The Plant Division assigns numbers to new Gaithersburg buildings when they are in the planning stage. All Gaithersburg buildings are numbered numerically in series as follows:

100 series - Administrative Buildings

200 series - Laboratory Buildings

300 series - Service Buildings

400 series - Temporary Buildings

500 series - NIST Annex Buildings

800 series - Local Leased Buildings

At Boulder, the Engineering, Maintenance and Support Services Division (EMSS) assigns numbers when new buildings are in the planning stage. Building numbers reflect the fiscal year construction begins and a sequential identifier.

b. Naming of Buildings

(1) Divisions occupying a building may propose a change to a building name to the Chief of Plant Division in Gaithersburg or the Chief of EMSS in Boulder. The Plant/EMSS Chief discusses the proposed building name with the principal organizational units occupying the building to determine acceptability. If a Boulder building, the name is also discussed with the Director of the Boulder site.

(2) If a new building, the Chief of Plant Division or the Chief of EMSS initiates a proposal for a building name. If a new Boulder building, the name is also discussed with the Director of the Boulder site.

(3) The acceptable building name is forwarded to the Chief Facilities Management Officer (CFMO) who submits the proposed name and abbreviation by memorandum to the Office of the Director for approval.

(4) The CFMO advises the following Divisions of newly approved names and abbreviations of buildings:

- Plant Division
- Administrative Services Division
- Emergency Services Division
- Engineering, Maintenance and Support Services Division
- Management and Organization Division
- Information Services Division
- Applications Systems Division

USE OF GROUNDS AND OUTDOOR FACILITIES

Sections

7.07.01 Purpose

7.07.02 Scope

7.07.03 Legal Authority

7.07.04 Policy

7.07.05 Delegations of Authority

7.07.06 Responsibilities / Approval Authorities

7.07.07 Requirements

7.07.08 Liability

7.07.09 Content Owner

7.07.10 Effective Dates

Appendix A - Requesting Use of Grounds and Outdoor Facilities for Sports and/or Social Activities

Appendix B - Obtaining Permission to Display Art Work on Building Corridor Walls and Doors

7.07.01 PURPOSE

This subchapter describes policies and procedures for use of the National Institute of Standards and Technology (NIST) grounds and outdoor facilities for sports and/or social purposes.

7.07.02 SCOPE

The provisions of this subchapter apply to all NIST facilities.

7.07.03

LEGAL AUTHORITY

DOO 30-2A

7.07.04

POLICY

a. The grounds and outdoor facilities at each NIST site may be made available to Institute employees, their families, and guests under certain conditions as outlined below in this section and 7.07.07 for sports and/or social use during specified hours on workdays, and all day Saturdays, Sundays, and official holidays. See Appendix A for procedures to request use.

In Gaithersburg, this may include the picnic grounds, softball fields, fishing ponds, etc.

b. The Institute reserves the right to deny permission for use of the grounds and outdoor facilities when the type of function is not considered one which should properly be held at a federal site.

c. In Gaithersburg, Institute grounds will not be made available solely for social or sports activity to outside groups such as charitable or civic organizations, religious or political groups, other federal agencies, or State and local governments.

In Boulder, unless requested and approved in accordance with the agreement between NIST, the City of Boulder, and the federally recognized American Indian Tribes, Institute grounds will not be made available solely for social or sports activity to outside entities such as charitable or civic organizations, religious or political groups, State and local governments, or federal agencies/groups that do not currently have a presence on the NIST Boulder campus.

d. Standards Employees Benefit Association (SEBA)-and Boulder Labs Employee Association (BLEA) sponsored athletic teams may use the grounds for intra-SEBA/BLEA games. Teams from other federal agencies and from private industry may be invited to play SEBA/BLEA teams on NIST grounds with the approval of the Chief, Emergency Services Division in Gaithersburg or the Site Manager in Boulder.

e. On scheduled federal workdays, Institute employees, NIST associates, members of their families, and a few guests may use the picnic site during the lunch period.

f. Building corridor walls and doors may be used to display suitable art work. See Appendix B for procedures. On the Gaithersburg campus, this does not pertain to the first floor of the Administration Building 101 or to the conferencing areas.

7.07.05

DELEGATIONS OF AUTHORITY

The Chief Facilities Management Officer and the Director, Public and Business Affairs Office jointly in Gaithersburg and the Site Manager in Boulder are responsible for carrying out the activities under this subchapter. The Chief Facilities Management Officer has delegated some of the approval authorities as outlined in sections 7.07.04 and 7.07.07.

7.07.06

RESPONSIBILITIES / APPROVAL AUTHORITIES

- a. The Director, Public and Business Affairs Office in Gaithersburg or the Site Manager in Boulder approve requests for use of the grounds after hours for picnics, sports, or social activities where there are to be more than ten in the group, including NIST employees.
- b. The NIST Director approves requests to consume beer, liquor, or wine on the Institute grounds (Gaithersburg and Boulder). These beverages may not be consumed without the NIST Director's express approval (Ref. 15 CFR 265.36). Requests should be forwarded to the NIST Director through the Chief Facilities Management Officer in Gaithersburg or the Site Manager in Boulder.

Information regarding NIST's drug-free workplace program is available on the HRMD website.

- c. OU Directors approve art work to be displayed by members of their staffs in the corridors of buildings in their assigned areas. See Appendix B for procedures.

7.07.07

REQUIREMENTS

- a. Children of employees and of guests must be under parental supervision at all times, and must not be permitted at the ponds alone or allowed to wander or play in any buildings. Children are not permitted on the grounds for sports or social activities unless accompanied by an Institute employee.
- b. In Gaithersburg, picnic fires are permitted only in the picnic grove east of the Administration Building. Either the permanently installed or portable braziers may be used. The user group is responsible for putting out the fire.

In Boulder, picnic fires are not permitted. If requested in accordance with the Programmatic Agreement between NIST and federally recognized American Indian Tribes, ceremonial fires may be approved and permitted by the Site Manager in Boulder.

c. In Gaithersburg, groups using the picnic grove east of the Administration Building may use the restroom facilities just off the lobby of the Administration Building.

In Boulder, groups using the grounds near the main entrance of Building 1 may use the restroom facilities off of the main lobby in Building 1.

d. All outdoor activities are to be terminated at dark (one-half hour after sunset).

In Boulder, if requested in accordance with the Programmatic Agreement between NIST and federally recognized American Indian Tribes, outdoor activities after dark (or one-half hour after sunset) may be approved and permitted by the Site Manager in Boulder.

e. Disposal of litter on Institute property is prohibited. Everyone using the Institute grounds is required to remove or dispose of all trash, paper, bottles, cans, etc., created by their own activity or the activity of their family or guests.

f. In Gaithersburg, fishing in the ponds is permitted with participation limited to NIST employees, their families, and guests. Fishing will be "Catch and Release Only". Fishing is at the risk of the parties involved. Anyone over 15 years of age must have a valid Maryland fishing license.

During scheduled federal workdays, fishing is permitted Monday through Friday from dawn (one-half hour after sunrise) until 8:30 a.m., at lunchtime (30 minutes to be taken between the hours of 11:30 a.m. and 2:00 p.m.), and after hours from 5:00 p.m. until dark (one-half hour after sunset). On weekends and federal holidays, fishing is permitted from dawn until dark. Ice fishing is prohibited.

g. Ice skating on the ponds is strictly prohibited.

h. Cross-country skiing is permitted on all grassy areas only after one or more inches of snow has accumulated. Skiing is prohibited on bare grass, on or within fifty feet of the ponds and buildings, and near or on cleared roadways. Skis must be removed and carried when crossing cleared roadways, when approaching the ponds (within fifty feet), or when entering any of the buildings.

Hours for participation are the same as for fishing (see paragraph f. above). Participants should check with the Police Services Group in Gaithersburg or the Site Manager in Boulder to find out if the grounds are open for cross-country skiing and in what areas.

i. Permission will not be granted to fly gasoline or other liquid fuel powered model airplanes, sail model boats, or use the grounds or parking lots for "gas buggies," trail bikes, and similar vehicles. Use of small, lightweight electric model airplanes must be cleared through the NIST Police. They will not be flown during business hours and must be kept at least 200 feet from buildings, parking lots and roadways.

j. Archery, and the shooting of firearms, CO2, BB, or air rifles and pistols, or the use of any other device that will expel or propel a projectile, such as a slingshot, spear gun, blowgun, etc. is strictly prohibited. Exceptions require approval of the Chief, Emergency Services Division in Gaithersburg or the Site Manager in Boulder.

k. In Gaithersburg, pictures or art work must be attached to pre-painted metal walls by magnets, which may be obtained from the Building 301 Storeroom. Under no circumstances may adhesives or adhesive tapes of any kind be used to place art work on the walls and doors since removal also takes off the pre-painted finish of the metal wall panels.

In Boulder, pictures and artwork must be on free-standing stands.

7.07.08

LIABILITY

a. Any individual permitted to use the Institute grounds for sports or social activity, does so at their own risk so far as injury to persons or damage to personal property is concerned. The Institute reserves the right to seek redress against any organized group, individual, or group of individuals for damage to Institute property resulting from sports or social activities on the grounds.

b. The Institute will not be financially responsible for any losses or damage to privately-owned art work displayed in the corridors. If the employee wishes to have art work insured, arrangements must be made with their own private insurance company.

7.07.09

CONTENT OWNER

Office of the Chief Facilities Management Officer

Chief, Plant Division

Chief, Engineering, Maintenance and Support Services Division

Director, Public and Business Affairs Office

7.07.10

EFFECTIVE DATE

August 31, 2009

APPENDIX A

REQUESTING USE OF GROUNDS AND OUTDOOR FACILITIES FOR SPORTS AND/OR SOCIAL ACTIVITIES

1. The picnic grove and the Administration Building 101 center courtyard may be scheduled for a sporting or social activity by contacting the Audio-Visual Services Group of the Public and Business Affairs Office on extension 3317.

2. Procedure for Small Groups (up to ten persons, regardless of the number of NIST employees.)

An employee may bring in members of their family and guests by signing them in at the Visitor Center or after hours at the Main Gate. The employee must remain with the family and guests while on the grounds. If the activity begins before 6:30 p.m. on workdays, the employee signs out members of the family or guests who leave after 6:30 p.m.

[Note: The employee sponsoring the group is responsible for ensuring that all adult foreign national guests (18 years and older) are registered in advance in accordance with Subchapter 14.03 Foreign Visitors. This includes completing the documentation required by DAO 207-12, "Foreign National Visitor and Guest Access Program."]

3. Procedure for Larger Groups (more than ten persons regardless of the number of NIST employees)

a. SEBA/BLEA and organizational units of the Institute wishing to use the grounds or facilities for group activities should request permission by sending a memorandum addressed to the Chief, Emergency Services Division in Gaithersburg or the Site Manager in Boulder.

b. Include the following in the memorandum:

- Date of planned activity
- Approximate times
- Area desired
- Sports planned (softball, baseball, fishing, other)
- Food and beverages planned (if wine, beer, or liquor will be consumed, specify how beverages would be controlled)
- Expected attendance
 - Names of employees

- Names and nationalities of guests)

[Note: The organization sponsoring the event is responsible for ensuring that all adult foreign national guests (18 years and older) are registered in advance in accordance with Subchapter 14.03 Foreign Visitors. This includes completing the documentation required by DAO 207-12, “Foreign National Visitor and Guest Access Program

- Statement that group accepts responsibility and will arrange for overseeing the activity of any children present

c. The memorandum asking permission should be initiated at least two weeks before the planned date of the activity or dissemination of any publicity regarding the activity.

d. For after hours, employees may arrange for visitor passes and either pick them up at the Visitor Center in advance during business hours, make arrangements with the Visitor Center for the pass to be available at the Gate House, or may sign in each visitor at the Gate House. The NIST Police encourage making advance arrangements.

e. If a request is made for the approval of alcoholic beverages, the memorandum should be addressed to the NIST Director through the Chief Facilities Management Officer in Gaithersburg or the Site Manager in Boulder. The Chief Facilities Management Officer in Gaithersburg or the Site Manager in Boulder will initial the memorandum to indicate endorsement of the request. Under Departmental regulations, only the NIST Director may give approval for the consumption of alcoholic beverages on the grounds.

f. Those securing the approval are responsible for the group maintaining proper decorum through the period of the activity.

APPENDIX B

OBTAINING PERMISSION TO DISPLAY ART WORK ON BUILDING CORRIDOR WALLS AND DOORS

1. An employee who wishes to display a work or works of art on building corridor walls and doors must obtain permission from the OU Director. Material placed on walls and doors without such approval will be removed.
2. Each picture, poster, exhibit, or other art work displayed must:
 - a. Have technical or artistic content related to the work, mission, or history of the organizational unit, or of the National Institute of Standards and Technology;
 - b. Be displayed in an orderly manner which will not detract from the appearance of the building; and
 - c. Be appropriate for a federal facility in the opinion of the OU Director.
3. To obtain permission to display art work, an employee should send a memorandum request to the OU Director through the Division Chief/Center Director. The memorandum request should describe the art work to be displayed, the proposed exhibit place, and the length of time the work is to be displayed.
4. The OU Director may ask to see the work before approving the display.
5. In Gaithersburg, the employee will use magnetic devices to attach the art work to the corridor walls and doors. Under no circumstances may adhesives or adhesive tapes of any kind be used to place art work on the walls and doors since removal also takes off the pre-painted finish of the metal partitioning. Devices for hanging small or large pictures may be obtained from the Building 301 Storeroom.

In Boulder, pictures and artwork must be on free-standing stands, and the employee is responsible for providing these stands. NIST is not responsible for the theft, loss or damage of free-standing stands.
6. The OU Director may ask the employee to remove the art work from the corridor walls and doors at any time.

NIST Administrative Manual
Subchapter 7.09

PRECIOUS METALS

Sections

7.09.01 Purpose

7.09.02 Scope

7.09.03 Policy

7.09.04 Definition

7.09.05 Responsibilities

7.09.06 Annual Inventory Procedures

7.09.07 Safeguarding Precious Metals

7.09.01

PURPOSE

This subchapter establishes guidelines for the accountability and control of precious metals at the National Institute of Standards and Technology.

7.09.02

SCOPE

The procedures contained in this subchapter apply to all NIST employees at Gaithersburg and Boulder sites.

7.09.03

POLICY

It is NIST policy that precious metals are accurately accounted for and controlled to safeguard against unauthorized use or theft. The inventory is controlled by formal inventory records and Accounting Classification Code Structure (ACCS) in the Commerce Business System (CBS).

7.09.04

DEFINITION

Precious metals include metals having a high monetary value in relation to their volume or weight, or condition status; new, used, consumed or embedded.

New: The stock of precious metals that has not been altered, and has retained its original properties and purity.

Used: Precious metals that have been used in experiments and are no longer pure. Although these metals had their original properties and/or purity altered, alternative future experiments still exist. This includes scrap metals that are scheduled to be transferred to excess.

Consumed: Pieces of metal that no longer exist in a form compatible for inventory purposes after the normal course of laboratory experiments or processing (e.g., gold used to coat an optical mirror). These include all precious metals placed or located in such a position as to be unavailable for recovery, or have been vaporized, dissolved, or converted in such a way as to be no longer recognized as a precious metal. These metals can no longer be accounted for and are considered “consumed”. The “consumed” totals must be reported to the Administrative Services Division (ASD) and Finance to adjust the precious metals inventory on hand in the Precious Metals Subsidiary Ledger.

Embedded: Precious metals that have been altered but have retained the original properties and purity. Precious metals that are used to construct thermocouples, fixed point crucibles, or other devices. The weight and value of the precious metals has been determined during the construction of the device. Embedded precious metals are metals that are not easily removed and or the process of recovery is too difficult for easy removal from the laboratory or site. The weight of the precious metal cannot be determined due to accessibility or location, or how it is used (e.g., enclosed in a graphite, quartz, alumina, and/or stainless steel container). Precious metals used under the “embedded” category are valued at historical cost. However, if the historical cost is not available, the market value will apply.

The precious metals include silver, gold, platinum, palladium, iridium, gallium, rhodium, osmium, and ruthenium. The latter six are less known than silver, gold, and platinum and are generally more valuable in terms of open-market price.

7.09.05

RESPONSIBILITIES

Each Division Chief is responsible for control, safeguarding, and accountability of precious metals in their division.

a. Division Chief

(1) Establishes and appoints an employee to handle the responsibilities for the security of precious metals in their custody and restricts access to appropriate personnel.

(2) Ensures job descriptions include custodial duties for precious metals and that each precious metals custodian is issued a copy of this subchapter.

(3) Provides Administrative Services Division (ASD) and the Finance Division with the names of the precious metal custodians and promptly notifies in writing when responsibility is transferred to other individuals. When responsibility is transferred to another precious metal custodian a joint inventory must be completed and stated on the letter appointing a new custodian. For new precious metals custodians, divisions are required to notify the Supply Technician in ASD's Logistics Group of changes to precious metals custodianship.

(4) Each division chief is responsible for combining the annual inventory reports from all custodians in the division and submitting one consolidated report through the division chief to Finance.

b. Precious Metal Custodian

(1) Oversees NIST employees' adherence to the precious metals procedures in order to account for, and safeguard, assets (per section 7.09.07 (b) and (c));

(2) Ensures that terminating and transferring employees have accounted for, and relinquished control of, precious metals in their custody by conducting a joint inventory. A precious metals clearance must be part of the Division's personal property clearance procedures for all terminating or transferring employees;

(3) Changes combination on containers that secure precious metals whenever custodian turnover occurs and reports the change to the local Office of Security;

(4) Conducts at least an annual inventory of all precious metals within the area of responsibility, after receiving instructions from the Finance Division and ASD and reports the results of the inventory to ASD by the required due dates;

(5) Reports promptly to ASD's Logistics Group any material expended in tests, or built, consumed or embedded into a piece of apparatus for another government agency, or otherwise consumed, which requires an adjustment to inventory records.;

(6) Promptly reports thefts, lost or missing precious metals to the Police Services Group (Gaithersburg) or DOC Police (Boulder); and submits a NIST Form 6A, "Request for Property Board of Review Action," to ASD's Logistics Group, with a copy of the Police report attached.

(7) Establishes practical limits for retention of surplus and related scrap beyond which appropriate disposal action is warranted. Excess scrap is transferred to ASD's Logistics Group or Boulder Property Management for disposition using NIST Form 81, "Intra-Office Transfer of Equipment," and a joint inventory is conducted between the precious metal custodian and the Property Accountability Officer. Prior coordination between the precious metals custodian and ASD's Logistics Group excess property team manager will be done prior to turn-in, transfer, or pick-up.

(8) Provides adequate facilities, training, and equipment for the security of precious metals in their custody. Precious Metals Custodians requiring refresher training are encouraged to contact the

Supply Technician in ASD's Logistics Group or ASD's Logistics Group Leader for refresher training.

(9) Monitors the acquisition of new precious metals. Consults with other division precious metals custodians within their Organizational Unit (OU) within their OU to determine whether precious metals are available within the division before placing a new order. The Person that placed a procurement action for precious metals notifies the appropriate division precious metals custodian of all precious metals acquisitions, indicating the staff responsible for the acquisition and the date of receipt. Ensures that precious metals which have not been utilized are transferred for disposal or reuse within the agency. This will prevent precious metals custodians from holding metals that are not used. The precious metals custodians must provide a copy of the requisition to ASD's Logistics Group for all precious metals ordered, transferred, shipped, or received. A control log must be maintained by each precious metals custodian to record the receipts, issues, transfers and balances of precious metals under their control.

(10) Bankcard Purchases for Gaithersburg and Boulder

(a) When entering your division Accounting Classification Code Structure (ACCS) information into CBS, be sure to select the correct Object Class Code, 26-48. The first two digits, Object Class Code 1, represent the purchase of goods. The second two digits, Object Class Code 2, represent the Precious Metals category. Use of an incorrect object class code affects the ability to track precious metals acquisitions.

(11) C-Request (Purchase Orders)

1. Gaithersburg

(a) When entering your division Accounting Classification Code Structure (ACCS) data, select the correct object class code, 26-48. The first two digits, Object Class Code 1, represent the purchase of goods. The second two digits, Object Class Code 2, represent the Precious Metals category. For each line item, provide point of contact (POC) information (name, division/group, telephone extension,) unless the complete order is for one person/division/group, and physical location where the item will reside. If the item ordered is for the use of a division other than the one placing the order, list the division/group that will own the item.

2. Boulder

(a) When requesting for precious metals all requisitions will be submitted to the local Boulder procurement agency, the correct object class code, 26-48,. The first two digits, Object Class Code 1, represent the purchase of goods. The second two digits, Object Class Code 2, represent the Precious Metals category. For each line item, provide point of contact (POC) information (name, division/group, telephone extension,) unless the complete order is for one person/division/group, and physical location where the item will reside. If the item ordered is for the use of a division other than the one placing the order, list the division/group that will own the item.

c. Administrative Services Division (ASD)

- (1) Establishes and maintains inventory records regarding precious metals and related scrap for both Gaithersburg and Boulder OUs. This procedure includes maintaining a (+) or (-) ten gram per metal group threshold for inventory accuracy within each division; and
- (2) Provides assistance to OUs in safeguarding precious metals as outlined in Subchapter 7.09.07.
- (3) Receives precious metals at NIST's ASD's Logistics Group in Building 301 in Gaithersburg and Building 22 in Boulder;

1. Gaithersburg

(a) For purchase order requisitions, ASD's Logistics Group forwards the #2 copy of the Receiving and Inspection (R&I) Report or Purchase Order (PO) to the division Administrative Officer (AO) to verify amount ordered and received, and to obtain the division precious metals custodian's or their designee's signature. The signed R&I Report or Purchase Order (PO) is forwarded to the Finance Division. ASD's Logistics Group hand delivers copies #1 and #3 of the R&I Report, along with the precious metals received, to the division precious metals custodian or other division representative. The #1 copy is signed by the receiving division precious metals custodian or other division representative, and is returned and retained by ASD's Logistics Group for its internal records. The #3 copy is maintained by the division precious metals custodian or division representative for their own accountability and records.

(b) For purchase card requisitions, ASD's Logistics Group hand delivers the precious metals received to the division precious metals custodian or other division representative. A copy of the R&I is signed by the receiving division's precious metals custodian or their designee, and then a copy of the R&I is returned and retained by ASD's Logistics Group for its internal records. The division precious metals custodian or division representative signs a copy of the "packing list" receipt and ensures that a copy is forwarded to ASD's Logistics Group to update the precious metals database for inventories on hand.

2. Boulder

(a) For purchase order requisitions, precious metals are received through the local Boulder Procurement and receiving agency (NOAA/MASC). A copy of the Receiving and Inspection (R&I) Report or Purchase Order (PO) is sent to the division Administrative Officer (AO) to verify amount ordered and received. The signed R&I Report or Purchase Order (PO) is forwarded to the Finance Division. The division precious metals custodian or division representative signs a copy of the receipt and ensures that a copy is forwarded to ASD's Logistics Group in Gaithersburg to update the precious metals database for inventories on hand.

(b) For purchase card requisitions, precious metals are received through the local Boulder Procurement and receiving agency (NOAA/MASC). A copy of the R&I is signed by the receiving division's precious metals custodian or their designee. The division precious metals custodian or

division representative signs a copy of the “packing list” receipt and ensures that a copy is forwarded to ASD’s Logistics Group in Gaithersburg to update the precious metals database for inventories on hand.

(4) Promptly transfers all scrap and excess precious metals;

(a) NIST employees in Gaithersburg transfer scrap and excess precious metals to ASD’s Logistics Group excess property team. A joint inventory of all amounts listed on the form NIST-81 is conducted by the division precious metals custodian and ASD’s Logistics Group excess property team manager, and both sign the precious metals transfer form. ASD’s Logistics Group excess property team manager calls the refining contractor to coordinate shipment date and the amount of the precious metals being shipped; prepares form NIST-386, Shipping Order; requests shipping labels; ensures ASD’s Logistics Group Leader authorizes the shipment by signature; takes the scrap and excess precious metals to ASD’s Logistics Group for shipment, and keeps a copy of the shipping documents with tracking number for division precious metals custodian records. In the event that scrap and excess precious metals are not shipped the same day they are received in ASD’s Logistics Group, they are secured in the Emergency Services Division’s vault until shipped. Seal tape is placed on the packages to prevent tampering and any alteration is reported to the Emergency Services Division and ASD’s Logistics Group Leader. When check payment is received from the refining contractor, ASD’s Logistics Group excess property team manager prepares a form NIST-766A, “Transmittal Sheet for Cash Collections,” and hand delivers the check and transmittal form to Finance’s Receivables Group. ASD’s Logistics Group excess property team manager provides a copy of all transfers/sales forms listed above to ASD’s precious metals custodian on all scrap and excess precious metals, in order to update the division’s precious metals inventory on hand balances.

(b) Boulder Property Management Office performs a joint inventory with the Boulder precious metals custodians of all amounts listed on the form NIST-81 by the division precious metals custodian and the property accountability officer, and both sign the precious metals transfer form. The property accountability officer calls the refining contractor to coordinate shipment and the amount of the precious metals that is being shipped; prepares the form NIST-386; requests shipping labels; ensures the division chief authorizes the shipment by signature; Takes the scrap and excess precious metal to the Shipping and Receiving Group for shipment; keeps a copy of the shipping documents with tracking number for division precious metals custodian records; send copies of all scrap and excess inventory shipped, shipping documents, and a copy of the check received to NIST Gaithersburg ASD’s Logistics Group excess property team manager. In the event the precious metals are not shipped the day received, they are secured in the office safe until shipped. A seal tape is placed on the packages to prevent tampering with the package, and any alteration is reported to Boulder, NIST Police, and the division chief. A copy of the report is sent to NIST Gaithersburg ASD’s Logistics Group excess property team manager and supply technician in ASD’s Logistics Group for their files. When check payment is received from the refining contractor, the Property Accountability Officer prepares the form NIST-766A and forwards the

form to the NIST Gaithersburg Finance Division. A copy of all scrap and excess precious metals transactions is sent to ASD's Logistics Group Leader to update the record of precious metals inventory on hand.

(5) The ASD's Logistics Group will provide training to precious metals custodians either in a class environment or one-to-one basis.

d. Emergency Services Division

(1) Reviews the report prepared by the Finance Division after each annual physical inventory to identify OU/Divisions that may require a storage compliance review.

(2) Verifies that items requiring special security are secured in accordance with Subchapter 7.09.07 below, and are contained in a GSA class 5 security cabinet which is, when applicable, connected to the NIST security alarm system with restricted access. A copy of the Police results is filed with the final precious metal inventory records.

(3) Provides temporary storage for precious metals while the OU/Division awaits the purchase and or installation of a GSA class 5 security cabinet.

(4) Provides guidance and security inspection in order to comply with NIST policies, and DOC and federal security regulations.

(5) Assists with the connection of security cabinets or rooms to the NIST security alarm system.

e. Finance Division (includes the Policy and Compliance Group, Office of the CFO)

(1) Reconciles the precious metals subsidiary ledger account with the annual report submitted by ASD's Logistics Group after the physical inventory is complete. Any discrepancies are resolved promptly between the Finance Division and ASD;

(2) Reviews operations and records of ASD's Logistics Group and other OUs to verify that proper procedures are being followed in managing and safeguarding precious metals and reporting inventory results;

(3) Initiates, coordinates, and observes a sample of annual physical inventories performed by precious metals custodians at NIST including Boulder OUs. The Boulder property accountability officer, may observe or will assist as per request from the Finance Division.

(4) Verifies inventory results with records maintained by ASD:

(5) Provides advice and assistance on record keeping of precious metals, including the issuance of a list to the Emergency Services Division of any OU/Division that may require storage compliance review, based on the completed dollar storage by OU/Division. This list will have each OU/Division and total dollar reported during the current inventory.

7.09.06

ANNUAL INVENTORY PROCEDURES

The Finance Division and ASD prepare and distribute a memorandum to notify division precious metals custodians that an inventory is required and the expected completion date.

a. Division

(1) Precious metals custodians are responsible for verifying that beginning balances are the same as previous inventory ending balances. New acquisitions, issues/consumptions and transfers are recorded in each division's precious metals inventory records (See paragraph (b) of section .07 of this subchapter). Precious metals custodians verify that precious metals issued are in the possession of the requestor in sufficient time to meet due dates;

(2) If the precious metals custodian, or their designee, conducting the inventory is unable to physically see the material, the employee accountable acknowledges possession by signature;

(3) Precious metals custodians are required to account for all precious metals in their division. Issues and receipt forms are to be recorded as per the instruction and example of section .07 of this subchapter, Safeguarding Precious Metals.

(4) Precious metals in control of the precious metals custodian shall be counted and verified in the presence of an independent second party observer prior to the submission of the required report to ASD's Logistics Group.

b. The following descriptions of precious metals must be used: new, used, consumed or embedded. All precious metals must be accounted for in one of these categories.

Note: Any out of balances listed above should be explained in the remarks section of the Inventory sheet. Examples are:

(1) Overages - recovered from equipment, or found during lab clean up.

(2) Shortages – Form NIST-6A, accompanied by the police report.

(3) Reclassification - 10 grams of pure gold reclassified to gold alloy (90% gold, 10% Silver.)

(5) Precious metal custodian prepares a report for submission to the division office. Each division chief combines the reports from all custodians in the division and submits one consolidated report through the division chief to Finance.

(6) Standard Reference Materials (SRMs) precious metals are considered as SRM inventory and are included in the SRM inventory rather than the division precious metal inventory.

c. ASD, Finance Division and Emergency Services Division;

(1) ASD and the Finance Division reconcile the physical inventory count after completion of the 100% precious metals physical inventory. Any discrepancies recorded in the precious metals subsidiary ledger or in the precious metals database are researched and corrected. As required, precious metals custodians provide additional information in order to correct any discrepancies found during this reconciliation.

(2) ASD adjusts precious metals inventory records for explained differences between the actual physical inventory reports and control records;

(3) ASD prepares a report to the Finance Division showing inventory results. The report should include an inventory summary sheet showing actual and book balances. All differences should be summarized on a separate report with explanations of unusual differences.

(4) The Finance Division provides a list to the Emergency Services Division of the OU/Division that may require storage compliance review, based on inventory value after the physical inventory is completed. The list includes OU/Division and total dollar reported during the current inventory.

(5) The Emergency Services Division verifies that items requiring special security are secured in accordance with section .07 of this subchapter, and are contained in a GSA class 5 security cabinet which is, when applicable, connected to the NIST security alarm system with restricted access. A copy of the police results are filed with the final precious metal physical inventory records.

(6) ASD's Logistics Group reports irreconcilable differences between the actual physical inventory and inventory control records to the Property Board of Review for necessary action.

7.09.07

SAFEGUARDING PRECIOUS METALS

a. Precious metals must be kept in a secured safe or cabinet locked by a combination lock when not in use, with access limited to the responsible precious metals custodian or designee.

The following guidelines are adopted by NIST for securing precious metals:

(1) Up to \$5,000 worth of precious metals should be contained in a lockable metal cabinet of sufficient size that one person would have extreme difficulty in moving the cabinet. Access should be restricted.

(2) \$5,001 to \$24,999.99 worth of precious metals should be contained in a metal file cabinet equipped with a bar and a hardened, tamper resistant padlock or combination lock, and of a sufficient size that two people would have extreme difficulty in moving the cabinet. Access must be restricted.

(3) When the precious metals in a cabinet, or multiple containers in the same location, exceeds \$25,000, all of the cabinets and containers should be contained in a GSA class 5 security cabinet

connected to the NIST security alarm system or the entire room must be connected to the NIST security alarm system with restricted access.

(4) In the event that emergency storage is required, the Emergency Services Division, or DOC Police in Boulder, can provide vault storage as a temporary solution. The Emergency Services Division can provide additional guidance and security inspection in order to comply with NIST policies, and DOC and federal regulations.

b. A control log must be maintained by each precious metals custodian to record the receipts, issues, transfers and balances of precious metals under their control. The minimum information contained in the document should be: item description, weight, name of borrower, dates borrowed and returned, weight when returned as “new, used, scrap”, and explanation of difference. This log facilitates the annual physical inventory and provides a written record of precious metals acquired and consumed for better control and accountability of precious metals inventory.

Precious Metal Control Log											
Division	192										
PM Custodian	F. Desiran										
Month Ending	3/31/08										
Precious Metal	Weight in	Name of	Date	Date	Weight in		Total Grams		Differences		
Description	Grams	Borrower	Borrowed	Returned	Grams		Returns	Explanation for	Out	In	
	OUT				New	Use	New,Use	Differences	Grams		Remarks
Pure Gold	15grams	G. Baugher	2/6/2007	3/15/2008	5	3		2 grams consumed in exp	2 grams		3 grams scrap
	5grams	A. Roman	6/27/2007	2/18/2008	0	5	5grams		0	0	
Platinum	45grams	G. Smitchu	6/6/2007	4/1/2008	15	10	35grams	10 grams lost	10 grams		NIST 6A will submitted
Pure Silver											

*** Note: The precious metals custodian has the option to enter additional information on their precious metals log; i.e. ID #, location of the item associated with the use or embedded precious metal, type of pm form “powder, wire, foil, shot, etc”

c. The responsible precious metals custodian or designee must obtain a receipt from each borrower when issuing precious metals for laboratory work. This form is used to verify amounts reported to the precious metals custodian at the time of the annual inventory. The receipt must contain the type of metal, weight, date, signature of the borrower, and location of the precious metal being used. This form is maintained on file and a copy is attached to the annual Precious Metals Inventory as back-up documentation. (See sample)

Issues precious metals;

Receipt for Issue of Precious Metals	
Division:	
Custodian:	
Precious Metal	Description:
Weight:	
Date Issued:	
Location of PM being used:	
Remarks	
Received By:	
(Signature)	
Borrower Name	(Print Name)

d. The responsible precious metals custodian or designee must maintain a copy of all returned forms from each borrower and precious metals being returned. These forms are used to verify amounts reported by the precious metals custodian at the time of the annual inventory. The return must contain the description of metals, weight, date, signature of the precious metals custodian, and the condition category of either “New”, “Used”, or “Scrap”. This form is to be maintained on file and a copy is attached to the annual Precious Metal Inventory as back-up documentation. (See sample)

Returns unused precious metals;

Return unused Precious Metals			
Division:			
Custodian:			
Precious Metal Description:			
Weight:			
Date Returned:			
Borrower name:			
Condition of precious metal	New	Use	Scrap
Precious Metal Custodian Remarks:			
Received By:			
(Signature)			
(Print Name)			

STRUCTURE AND RESPONSIBILITIES

Sections

8.01.01 Purpose
8.01.02 Scope
8.01.03 Policy
8.01.04 Background
8.01.05 Overview
8.01.06 Responsibilities
8.01.07 Release of Information
8.01.08 References
8.01 Appendix A - Financial Event Schedule - pg. 1
8.01 Appendix A - pg. 2
8.01 Appendix A - pg. 3

8.01.01

PURPOSE

This subchapter describes general policies and responsibilities concerning the NIST financial management structure.

8.01.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

8.01.03

POLICY

It is NIST policy to practice sound financial management and establish and maintain procedures in compliance with Office of Management and Budget (OMB), Department of Treasury, General Accounting Office (GAO), Federal Accounting Standards Advisory Board (FASAB), Department of Commerce (DoC) directives and standards, and other federal legislation.

8.01.04

BACKGROUND

The Budget and Accounting Procedures Act of 1950 directed the Comptroller General to prescribe accounting principles, standards, and related requirements for executive agencies. Subsequent to passage of that Act, the General Accounting Office (GAO) issued accounting standards. However, due to a constitutional question of whether the legislative branch can issue and audit against such standards for the executive branch, agreement was never reached on accounting standards. As a consequence, accounting procedures and systems evolved inconsistently across agencies. In addition, financial audits have been subject to varying and conflicting interpretations of the accounting standards.

Since 1980, Congress has placed considerable re-emphasis on the need for federal agencies to establish and support improved accounting standards and principles in an effort to provide uniform financial reporting within the federal government. Legislation has been enacted requiring agencies to have systems that integrate budget and financial information based on consistent accounting and systems standards. In addition, long-range financial planning, audited financial statements, and development of cost information are required. The position of Chief Financial Officer is mandated at the levels of Office of Management and Budget (OMB) and executive agencies such as the Department of Commerce; these positions establish a financial management leadership structure within the executive branch. Legislation has also mandated more efficient collection of debts owed to the United States and calls for prompt payment of bills owed by the federal agencies. The Federal Accounting Standards Advisory Board (FASAB), which works under the general oversight of the Comptroller General, the Secretary of the Treasury, and the Director of OMB, was established in 1990; the Board has issued eight financial accounting standards. As a result of these still evolving laws and standards, federal financial management is in a state of change. Efforts are underway to implement transaction-based, integrated financial systems. Reporting requirements are changing and increasingly require linking of financial data to program performance measurements.

New roles and responsibilities are being defined within agencies. It has become increasingly important that employees have the skills and training required to keep pace with changes in technology and the developments in federal financial management. The Joint Financial Management Improvement Program (JFMIP) and the Chief Financial Officers Council have worked together to produce core competency documents for several types of employees involved in financial management. These documents describe necessary skills and abilities for entry- and mid-level personnel as well as senior managers and supervisors and specialized knowledge required for areas such as management analysts, financial specialists, financial system analysts, and information technology personnel.

8.01.05

OVERVIEW

Funding for activities at NIST comes from appropriations, reimbursements from other federal agencies, state and local agencies, the public, and a Working Capital Fund corpus.

The majority of work at NIST is funded by three direct Congressional appropriations: Scientific and Technical Research and Services (STRS), Industrial Technology Services (ITS), and Construction of Research Facilities (CRF). The STRS appropriated funds are focused on infrastructural technologies such as measurements, standards, evaluated data, and test methods for use by industry in commerce. ITS funds support cost-shared research by individual companies or industry-led joint ventures as well as providing a nationwide network of manufacturing extension centers integrated with federal, state, local, and private-sector programs in support of U.S. competitiveness. CRF funding is appropriated for safety and scientific functionality in existing laboratory space and construction and renovation of space. (See Subchapter 8.03, Budget Formulation, and Subchapter 8.04, Appropriated Funds.)

The reimbursable funds at NIST come from a variety of sponsors and support research in areas related to those funded by the appropriations (see Subchapter 8.05, Federal Government/Non-Federal Government/ CRADA-Sponsored Work for more information.) In addition, NIST performs calibrations and tests on a reimbursable basis, sells Standard Reference Materials (SRMs), and provides services between divisions within NIST through interdivision services arrangements (see Subchapter 8.06, Expense and Income Activities).

The NIST Working Capital Fund provides for initial funding for expense and income-supported activities, distribution of indirect costs as overhead, investments in equipment and inventories, and production of SRMs. NIST does not receive a separate appropriation for salaries and expenses of administrative personnel. Instead each source of funding contributes a share via surcharges to support these costs. As a result, each funding source pays a proportionate share of administrative costs. (See Subchapter 8.07, Working Capital Fund Programs.)

NIST uses project cost accounting to track the costs of activities funded by the various sources (see Sub-chapter 8.08, Cost Accounting). Cost centers are established to accumulate the costs. Each cost center is associated with only one source of funding and one program code. The last three digits of the seven-digit cost center number indicate the source of funding according to the cost center funding structure which has been established (see Subchapter 8.02, Fund Structure). Information about the cost centers is maintained in the NIST accounting system and is available for management use.

Financial management activities for a least three different year's budgets are going on simultaneously. While the current fiscal year (CY) budgetary resources are being used (executed), the formulation and review process for the next fiscal year or budget year (BY) is also occurring. Early in the CY, financial reviews and reports of prior-year (PY) activities occur, and by the middle of the CY, the formulation process has begun for the next budgetary year (BY+1). Additional details can be found in the Strategic Planning and Budget Calendar or in the Handbook on Budget Preparation and Resource Allocation (the "Color Book"). Both are issued annually by the Budget Division.

8.01.06

RESPONSIBILITIES

Specific financial management responsibilities to ensure appropriate administrative control of funds are found in Subchapter 8.04, Appropriated Funds.

a. NIST Director - The NIST Director determines the financial policies of NIST and directs the development and execution of its financial management programs.

b. Deputy Chief Financial Officer - The NIST Deputy Chief Financial Officer and Deputy Director for Financial Services serves as the senior financial management advisor to NIST management and is responsible for planning and oversight of all financial management activities and operations at NIST.

c. Budget Division - Facilitates the acquisition of appropriated funding and ensures that resources are utilized in accordance with Congressional intent and all pertinent regulations and policies. This includes the preparation, presentation, justification, and execution of the NIST budget as well as resource allocation and periodic analysis and reports to management on solvency and other financial issues.

d. Financial Management Systems Division - Provides oversight and management of centrally developed financial management systems and the implementation of such systems across NIST. This includes analysis and recommendations for new systems and modifications to existing systems to meet internal and external requirements.

e. Financial Operations Division - Administers the NIST and FARS system of accounting and provides accounting and other financial management services for other Departmental bureaus. The division provides advice on financial matters to the NIST Deputy Chief Financial Officer and to management at all levels of the serviced bureaus.

f. Financial Policy Division - Responsible for preparing financial reports and analyzing and developing improved financial policy.

The Financial Operations Division and the Financial Policy Division share responsibility for: managing a comprehensive accounting and financial program to provide for accountability of assets and accurate financial reporting; implementing effective internal controls; ensuring accurate data for financial reporting and certifying the official accounting records and reports; providing adequate financial data for management purposes; and providing advice on financial matters to the NIST Deputy Chief Financial Officer and providing input to the Department on financial procedures and reporting requirements.

e. Senior Management Advisors - The Senior Management Advisor directs the financial management activities within their OU. In particular, the Senior Management Advisor recommends resource allocations based on the OU management priorities; establishes operational plans based on OU management's resource allocations; monitors resource utilization by organizational units to ensure that resource allocations are not exceeded and that research program/service opportunities are not lost due to under-utilization of allocated resources. The Senior Management Advisor identifies funding problems; develops viable corrective actions; and implements OU management decisions. In addition, the Senior Management Advisor is a principal contributor to the formulation of NIST-wide financial management policy and responds to inquiries and answers questions of external organizations such as Congress, OMB, GAO, and the Inspector General regarding financial management activities and policies of the OU/NIST.

8.01.07

RELEASE OF INFORMATION

a. To ensure consistency and accuracy, all budgetary estimates or actual resource numbers, both dollars and personnel, which are to be reported outside of NIST, must be cleared through the Deputy Chief Financial Officer before release.

b. The nature and amounts of the President's budget decisions are confidential and will not be released until the budget is transmitted formally to Congress. The executive branch communications that have led to the budget will not be disclosed either by the agencies or by those who have prepared the budget.

8.01.08

REFERENCES

a. NIST Administrative Manual Subchapter 9.02 - Functional Statements.

b. NIST "Color Book" - The Annual Handbook on Budget Preparation and Resource Allocation, prepared by the Budget Division.

c. Chief Financial Officers Act of 1990 (P.L. 101-576) - The CFO Act requires long-range financial planning, audited financial statements, integration of budget and accounting data, and development of cost information. It also establishes the financial management leadership structure within OMB and federal agencies.

d. Debt Collection Improvement Act of 1996 (P.L. 104-134) - The Debt Collection Improvement Act significantly changed the way the federal government collects debt. The Act requires agencies to refer delinquent debt to the Department of Treasury after 6 months; Treasury is required to use more computer matching so that those who owe money to the government are not simultaneously being sent checks by the government; and it permits Treasury to deduct delinquent debt from government payments such as tax refunds, wages, and retirement and benefit payments.

e. Federal Financial Management Improvement Act of 1996 (P.L. 104-208) - The Federal Financial Management Improvement Act requires that each agency implement and maintain financial management systems that comply with federal requirements, applicable federal accounting standards, and the Standard General Ledger at the transaction level.

f. Federal Managers Financial Integrity Act of

1982 - (P.L. 97-255) - The Federal Managers Financial Integrity Act amends the Accounting and Auditing Act of 1950 to require federal agencies to establish internal accounting and administrative controls to prevent waste or misuse of agency fund or property and to ensure the accountability of assets.

g. Government Performance and Results Act of 1993 - (P.L. 103-62) - The Government Performance and Results Act is intended to bring about fundamental changes in the way government programs and operations are managed and administered. It requires agencies to prepare strategic plans and annual performance plans, as well as annual program performance

reports to the President and Congress beginning with FY 1999. It mandates a link between program performance and budgeting.

h. Prompt Payment Act (P.L. 97-177) - The Prompt Payment Act calls for payment of bills not later than due dates based on the receipt of proper invoices and satisfactory performance, as well as payment of any interest and penalties. The Act also stresses the importance of taking cash discounts.

i. Taxpayers Relief Act of 1997 - The Taxpayer's Relief Act requires federal accounting systems to produce IRS Form-1099 for payments for services over \$600 to corporations, in addition to earlier requirements that they be produced for payments to individuals.

FUND STRUCTURE

Sections

8.02.01 Purpose

8.02.02 Scope

8.02.03 Legal Authority

8.02.04 Policy

8.02.05 Delegations of Authority

8.02.06 Definitions

8.02.07 Responsibilities

8.02.08 Procedures

8.02.09 Content Owner

8.02.10 Effective Dates

Appendix A – Project Funding Structure

Appendix B – Explanation of Project Funding Structure

Appendix C – NIST Budget/Program Structure

Appendix D NIST Budget/Program Codes

Appendix E – National Science Foundation and Field of Science Codes

8.02.01

PURPOSE

This subchapter describes the funding structure of the National Institute of Standards and Technology (NIST) and the appropriate use of and procedures for establishing and coding projects.

8.02.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

8.02.03

LEGAL AUTHORITY

Title 31 of the United States Code (Money and Finance), specifically:

--Sections 1301, 1341-1342, 1349-1351, 1511-1519

--Sections 1101, 1104-1108, 1112, 3324

--Sections 1501-1502

Federal Managers' Financial Integrity Act (FMFIA) of 1982

OMB Circular A-11

OMB Circular A-123

DoC Accounting Principles and Standards Handbook

DoC Budget and Program Analysis Handbook

8.02.04

POLICY

NIST costs associated with a particular function must be accurately charged to the funding provided for that purpose. Costs are collected and recorded in approved projects in the Commerce Business System (CBS).

8.02.05

DELEGATIONS OF AUTHORITY

a. The Director has delegated administrative control of NIST appropriated funds to the NIST CFO, who has re-delegated to the Chief of the Budget Division and to the Chief of the Finance Division respectively the following duties:

- (1) Developing financial management systems and procedures consistent with the requirements of the DoC Budget and Program Analysis Handbook
<http://www.osec.doc.gov/bmi/budget/Budget%20Handbook.htm>
and DoC Accounting Principles and Standards Handbook;
<http://www.osec.doc.gov/ofm/Accounting/cover.html>

In addition, the CFO has re-delegated to the Chief of the Budget Division the following duties:

- (2) Allocating funds to heads of Operating Units (OUs);
- (3) Ensuring that operations are maintained within the limits of approved apportionments, financial plans, and operating budgets; and
- (4) Providing notification to appropriations committees and obtaining proper clearances prior to proceeding with reprogramming actions.

b. The Chief Financial Officer (CFO), in cooperation with the Chief of the Budget Division and the Chiefs of the Finance Division and Business Systems Division, is responsible for developing procedures to provide financial and employment data needed for administrative control and

reporting requirements and for maintaining liaison with the DoC Office of Budget and the Office of Financial Management on resolution of problems.

(1) Specific responsibilities of the Chief of the Budget Division are as follows:

- (a) Preparation of apportionment and reappropriation requests and supporting documentation, and periodic reports and other required data;
- (b) Allocation of budgetary resources to OUs in support of the programmatic distribution of funds appropriated by Congress, apportionments approved by OMB, and decisions by the NIST Director;
- (c) Issuance of operating budget reports to OUs and divisions reflecting the programmatic distribution of funds appropriated by Congress; and
- (d) Clearance and/or preparation and release of financial data from official records in response to miscellaneous external requests for information.

(2) Specific responsibilities of the Chief of the Finance Division are as follows:

- (a) Organizing, planning, developing, coordinating, and managing a comprehensive accounting/finance program for NIST; and
- (b) Certifying the accuracy of official accounting records and reports.

(3) The Director has delegated administrative control of maintaining a financial management system to the NIST CFO, who has redelegated to the Chief Business Systems Division who delegated responsibility for maintaining a financial management system that produces reports which show accrued costs, total obligations, unobligated balances, and total budgetary resources available to NIST.

c. The NIST Director has delegated authority to the OU Directors and Chief Officers to establish division operating budgets and project authorizations and to ensure that operations are maintained within limits of allocations issued by the Budget Division.

8.02.06

DEFINITIONS

a. Projects/Tasks – Projects are the building blocks in the Commerce Business System (CBS). Obligation and accrued cost transactions are charged to projects, which are the lowest level at which costs incurred are systematically recorded. A project is a seven-digit account that records all of the funding structure elements associated with an activity. The funding structure elements are project code, task code, project type, fund code, program code, NSF code, Field of Science (FoS) code, project leader, created by organization, work site, and budget initiative number. The first three digits of the project code identify the owning organization of the project. The fourth digit of the project code is an optional designator for use by the OU. The last three digits of the project code identify the source of funding that supports the work. Each distinct seven-digit

project also has an adjunctive three-digit alpha-numeric field that represents an activity related to the project code called the task. The task allows information to be broken down to a finer level of detail. All projects must have at least one task, and the default is 000. New project-tasks and changes to existing project-tasks are made on the CM004, Project Code Maintenance Screen. The latest procedure detail and the schedule to be followed in the establishment of projects in the Project Code Maintenance Screen can be found in the Finance Administrative Bulletin issued annually on the NIST Systems, News, Applications, and Procedures (SNAP). Step by step instructions for the CM004 can be found on the SNAP website.

b. Project Authorization – Budget Operating Plan (BOP) (FM066) To request project authorization after the start of a fiscal year or to request a change to the project, a requesting OU prepares a Budget Operating Plan (BOP) that is established in the CBS system to authorize the spending of project dollars at specified quarterly levels. A BOP is sent by the OU Administrative Officer to the Budget Division through the OU Senior Management Advisor (SMA), except for federal government, non-federal sponsors, CRADA, and gifts and bequests projects. For these excepted projects, the SMA approves the BOP based on firm financial backing information for the project received from the Finance Division. New BOPs and changes to existing BOPs are made on the FM066, Budget Operating Plan Screen. Instructions for completing a BOP are given in Appendix C. The latest procedure detail and the schedule to be followed in requesting authorization of projects for the start of the fiscal year is found in the Finance Administrative Bulletin issued annually. Step by step instructions for the FM066 can be found on the SNAP website.

8.02.07

RESPONSIBILITIES

- a. The Business Systems Division is responsible for establishing and modifying a project funding structure that meets NIST's needs and requirements.
- b. The Budget Division is responsible for requesting the four-digit establishment of fund codes and for establishing budgetary resources in the Budget Execution Modules in the CBS for all sources of financing with the exception of federal government, non-federal government, gifts and bequests, and Cooperative Research and Development Agreements (CRADAs).
- c. The Finance Division's Receivables Group is responsible for the review and approval of projects used for federal government and non-federal government-sponsored work, as well as CRADAs.
- d. Organizational Units (OUs) are responsible for establishing and properly coding projects.

8.02.08

PROCEDURES

- a. Establishment of Projects - Project Code Maintenance Screen (CM004)

- (1) New project-tasks and changes to existing projects are made on the CM004, Project Code Maintenance Screen. Access to the CM004 is via the Core Financial System

(CFS). The CM004 contains the following fields: Project Code, (Project) Title, (Project) Type, Fund Code, Program (Code), Field of Science Code, NSF Code, Goal Code, Project Leader, and Budget Initiative No. This screen establishes all of the accounting elements necessary for the project to become a data element in the CBS system.

(2) The steps to updating the CM004 are as follows:

- (i) The user (usually the Administrative Officer (AO)) enters the project and task information on the CM004.
- (ii) For all fund codes (FCs) except FC 0008 Advances and Reimbursements, the user approves the project on the CM004. All new FC 0008 Advances and Reimbursements projects must be approved by the Finance Division, Receivables Group.
- (iii) For all fund codes except FC 0008 Advances and Reimbursements, the SMA activates the projects on the CM004. All new fund code 08 projects must be activated by the Finance Division, Receivables Group.

(3) Key CM004 Points:

- (i) Projects are for all years and should remain active.
 - (ii) For Fund Code 08 projects, the Sponsor Code should be entered in the Budget Initiative Number field.
 - (iii) Once all data elements have been entered, save the project by using the save icon on the toolbar.
 - (iv) The Finance Division, Reimbursables Group approves and activates all Fund Code 08 projects.
 - (v) The rights to approve and activate the CM004 are requested by the SMA for his/her OU from the Budget Division.
- (4) Important startup procedures and information related to Project and Budgetary Set-Up for the current Fiscal Year and all future fiscal years can be found in the NIST Administrative Bulletin.
- (5) Seven (7) fields cannot be changed on the CM004 after the project has been approved. These are Bureau Code, Project Code, Fund Code, Program Code, D/R Flag, Effective Date (Beginning), and Approved By and Date.
- (6) Information on each of these fields on the CM004 can be found in the User Procedures found on the CBS Portal.

b. Authorization of Projects – Budget Operating Plans (BOPs) (FM066)

(1) The procedure and schedule to be followed for requesting authorization of projects for the start of the fiscal year is explained in the Administrative Bulletin issued annually. For FY 2010, the Start of Year Processes Timeline is as follows:

(2) To request authorization of a project after the start of the fiscal year or to request a change, termination, or deletion of a project, the requesting OU prepares a CBS FM066 screen (Budget Operating Plan) known as a BOP through the CBS Portal. An authorization is established on the FM066 – Budget Operating Plan (BOP) Transaction Screen accessed through CBS. The system does not require that a BOP be created in order to charge a project-task. The FM066 screen consists of two data entry tabs and two lookup tabs. The Budget Control Tab allows the user to enter the Accounting Code Classification System information for the quarterly authorization amount for a transaction. Additional information about the BOP can also be entered in the Notes section of this screen. Changes to approved BOPs are made by selecting Change and entering a code or reason for the change. The Budget Detail tab enables the user to enter the distribution of the authorization amount by effective date, amount, and object class. The quarterly transaction amounts on the Budget Detail must match the quarterly amounts on the Budget Control. The available allotment pool for the program code and quarter can be viewed on the Budget Detail. The Summary by Details tab summarizes the information entered on the Budget Detail tab. This information can be viewed for the entire Budget Operating Plan or just the current transaction. This tab is for viewing only and requires no data input from the user. The Summary by Objects tab summarizes the information entered on the Budget Detail tab by object class. This information can be viewed for the entire Budget Operating Plan or just the current transaction. This tab is also view only and requires no input from the user.

(3) Step by step instructions for each field on each of the tabs mentioned above can be found in the FM066 User Procedures found on the CBS Portal. This includes instructions for both a newly established BOP and a modification or CHANGE BOP.

(4) Important new procedures and information related to Project and Budgetary Set-Up for Fiscal Year 2010 and all future fiscal years can be found in the NIST Administrative Bulletin.

c. Key FM066 Points

- (1) If a project is not showing up in the ACCS List of Values when entering a BOP, the project and/or task may not be approved and/or activated on the CM004. Another cause could be that no allotment pool has been recorded by the Budget Division for the program code associated with the project-task.
- (2) If you receive the message that no pool is available, this indicates that no allotment pool has been recorded for the program code associated with the project-task. Users should contact their Budget Analyst to assist with this situation.

- (3) Two (2) start of year reports are available to compare with the allocation memos distributed from the Budget Division:

Start of Year: NSTBOP (CBS) – BOP Listing Report

Start of Year: NSTPROJD (CBS) – Project Listing Report

d. Additional CM004 and FM066 Resources

Additional Resources for the CM004 and the FM066 include the Customer Interaction Center (CIC) available for assistance Monday-Friday from 8:30 AM – 6:00 P.M. via phone at 301-975-5375 or by email at cic@nist.gov.

- (1) New procedures and information related to Project and Budgetary Set-Up for Fiscal Year 2010 can be found in the NIST Administrative Bulletin.

- (2) Specific training requests for CM004 and/or FM066 may be made through the CIC. Specific system input instructions for both the CM004 and FM066 input screens are contained on the SNAP website, under Project Maintenance and Authorization.

8.02.09

CONTENT OWNER

The Content Owner of Chapter 8.02 is the NIST Budget Division.

8.02.10

EFFECTIVE DATES

September 10, 2009.

APPENDIX A

PROJECT FUNDING STRUCTURE

(pertains to the last three digits of the 7-digit project number)

001-299 Scientific and Technical Research and Services (STRS)

001-299 STRS

300-349 Industrial Technology Services (ITS)

300-305 ITS OU reserve (base projects not authorized to accept charges)

306-340 ITS projects (base)

341-349 ITS projects (nonbase)

NOTE: 875-889 is also used for ITS nonbase projects

350-359 Undefined

360-364 Gifts and Bequests

365-369 Cooperative Research and Development Agreements (CRADA)

370-569 Federal Government Sponsors (other than expense and income projects)

570-579 Non-Federal Government Sponsors (other than expense and income projects)

570-574 State and Local Government and Nonprofit Organizations

575-579 Foreign Government and Public

580-699 Expense and Income and Interdivision Services

580-584 Seminars and Fee-Supported Conferences

585-594 Miscellaneous services

585-590 Federal Government

591-594 State, Local, and Foreign Government and Public

595-599 Interdivision Services

600-654 Calibration and Testing

600-629 Calibration - Public and Government

630-644 Testing - State, Local, and Foreign Government and Public

645-654 Testing - Federal Government

655-674 Standard Reference Materials Program Surcharge-Supported Activities and

Sales

655-660 SRM Program Operations

661-665 SRM Sales

666-674 SRM Service Development Support

675-679 Proprietary Measurements

680-684 Calibration Program Surcharge-Supported Activities

680 Calibration Program Operations

681-684 Calibration Service Development Support
685-699 Seminars and Fee-Supported Conferences

700-799 Standard Reference Materials - Production

800-849 Working Capital Fund Invested Equipment (IE)

800-809 Direct purchase of IE
800-805 Discretionary IE allocation
806-809 Initiative related/special IE allocation
810-849 Manufacture of IE
810-844 Discretionary IE allocation
845-849 Initiative related/special IE allocation

850-874 Construction of Research Facilities (CRF)

850-851 CRF OU reserve (base projects not authorized to accept charges)
852-854 CRF operating projects (base)
855-874 CRF projects (nonbase)

875-889 Industrial Technology Services (ITS - nonbase)

(NOTE: 341-349 is also used, see previous page)

890-899 Unassigned

900-919 Laboratory and Division Overheads

900-909 Division Overhead - Equipment Loan Repayment
910-919 Laboratory Overhead

920-949 Budget Division Use

920-939 Storeroom inventories
940-949 Miscellaneous

950-990 Institutional Support

950-974 Institutional Support operating projects (controllable base)
975-978 Institutional Support operating projects (controllable nonbase,
source: OU reserve)
979 Institutional Support operating projects (controllable nonbase,
source: NIST Director's reserve)
980-989 Institutional Support operating projects (uncontrollable)
990 Special agency-wide Institutional Support activities

991-999 Deputy Chief Financial Officer Use

Example of Project Number 810 9 (or alpha) 101
OU/Division (The first three digits must reflect the NIST Division).
Optional use by OU/Division (This can be alpha or numeric - digits/alphas)

of choice.)

Funding Source (recommended sources are below – if deviating from this listing, you must obtain the consent of the approving office. In the case of Other Agency projects, all Other Agency projects must use the designations below in determining the last three digits of the project that represent the funding source.

The source of support designations listed below indicates how projects are grouped and totaled on accounting and budget reports.

Projects

Source of Support

Appropriations

001-299	Scientific and Technical Research and Services
300-349, 875-889	Industrial Technology Services
350-359	Undefined
850-874	Construction of Research Facilities

Gifts and Bequest and Cooperative Research and Development

360-364	Gifts and Bequests
365-369	Cooperative Research and Development

Reimbursable Activity

370-569	Federal Government Sponsors
570-579	Non-federal Government Sponsors
580-584	Seminars and Fee-Supported Conferences
585-594	Miscellaneous Services
600-654	Calibration and Testing
655-660, 666-674	Standard Reference Materials Surcharge-Supported Activities
675-679	Proprietary Measurements
680-684	Calibration Program Surcharge
685-699	Seminars and Fee-Supported Conferences
700-799	Standard Reference Materials - Production

Equipment

800-809	Direct Purchase of WCF Invested Equipment
810-849	Manufacture of WCF Invested Equipment

Overheads

900-919	Laboratory and Division Overheads
---------	-----------------------------------

Institutional Support

950-990

Institutional Support

Miscellaneous

595-599

Interdivision Services

661-665

SRM Sales

920-939

Storeroom Inventories

940-949

Miscellaneous

991-999

Deputy Chief Financial Officer Use

APPENDIX B

EXPLANATION OF PROJECT FUNDING STRUCTURE

Appropriations

STRS, ITS, and CRF funds are appropriated annually to NIST. Usually, these funds are "no-year" appropriations (i.e., funds are available for obligation beyond the year in which they are appropriated). Specific guidelines for the carryover of funds from one fiscal year to the next are outlined in Subchapter 8.04, Appropriated Funds. For administrative convenience, the projects for these appropriations are divided into the following series:

001-299 Scientific and Technical Research and Services (STRS) - funding for NIST intramural programs.

--001-299 - STRS

Projects (Base) - "Base" funds are allocated to an OU Director for the accomplishment of OU objectives, consistent with the budget as approved by the Congress. Funds may be transferred to other NIST OUs or within the same OU by either a base or nonbase transaction. The "Base" level of an organization is considered to be the previous year's base allocation, adjusted for any cost of living, programmatic, or other adjustments in the appropriation and any internal assessments or approved reprogramming actions (see Subchapter 8.04).

Projects (Nonbase) - "Nonbase" refers to funds allocated to an OU for the current fiscal year only and does not represent an allocation that the OU would expect in succeeding years. Examples include unobligated balances from prior fiscal years, transfers of funds from other OUs, and one-time allocations from the Director's Reserve.

300-349 and 875-889 Industrial Technology Services (ITS) - Funding for NIST extramural programs.

--300-305 - ITS OU Reserve

--306-340 - ITS Projects (Base)

--341-349 - ITS Projects (Nonbase)

--875-889 - ITS Projects (Nonbase)

See explanations of numbering series types above.

850-874 Construction of Research Facilities (CRF) - Funding for construction, major renovations, modifications, and improvements.

--850-851 - CRF OU Reserve (Base)

--852-854 - CRF Projects (Base)

--855-874 - CRF Projects (Nonbase)
See explanations of numbering series types above.

350-359 Undefined

360-799 Reimbursable Activity

NIST's unique measurement capabilities and services are made available to outside customers based on criteria and procedures identified in Subchapters 8.05, Federal Government/Non-Federal Government/CRADA Sponsored Work and, subchapter 8.07 Working Capital Fund addresses Expense and Income Activities. NIST is authorized to charge for the full cost of services provided, including all overheads or indirect charges.

Use Surcharge - In addition to NIST out-of-pocket costs, non-federal customers also pay a share of building depreciation and Departmental overhead, levied as a use surcharge against the direct labor and personnel benefits cost of doing the work. Use surcharges collected are used for building maintenance and repair

360-364 Gifts and Bequests

Gifts and bequests are accepted from private sources for the purpose of aiding or facilitating the work of NIST. Funds assigned in this series must be clearly intended as a gift by the offeror. The distinguishing features of a gift are that the funds be transferred gratuitously and be free from restrictions, limitations, or control by the donor. However, the gift may be designated for a specific investigation or line of research or development. Generally, there is no timetable for performing work, and there is no reporting, accounting, or other "consideration" required of NIST. ("Consideration" is a distinguishing feature of a contract or agreement and is something of value which passes between the parties, e.g., the private organization or individual expects to obtain an advantage, right, profit, or service from the funds transferred to NIST.). Information concerning the acceptance and use of gifts is included in Subchapter 8.10.

365-369 Cooperative Research and Development Agreements (CRADA) - Use surcharge applied.

This series of project numbers is used to record costs, obligations, and contributions from NIST sponsors that pertain to the various consortia, CRADAs at NIST. Consortia and CRADAs may be financed by private industry, other federal agencies, or a combination of both for the advancement of scientific and technical knowledge. All deposit accounts should be established in this series regardless of dollar level. Once the agreement has been accepted, the Finance

Division automatically bills the amount specified in the consortium or CRADA. The recovery of a use surcharge is required for work done in this series. Information on procedures is included in Subchapter 8.05.

370-569 Federal Government Sponsors (other than expense and income projects)

This series includes various types of work done for other-federal-agency sponsors. It includes research and development as well as technical services. It is mainly for orders of \$25,000 and above, which must be accepted by the Finance Division. Orders above \$5,000 but less than \$25,000, may be included in this series if automatic billing is desired. Calibration work is not included in this series. Once the project has been established, the Finance Division automatically bills according to the terms of the agreement. Information on procedures is included in Subchapter 8.05.

570-579 Non-Federal Government Sponsors (other than expense and income projects) - Use surcharge applied

This series includes various types of work done at NIST for sponsors other than federal government agencies. It is mainly for orders of \$25,000 and above, which must be accepted by the Finance Division. Orders above \$5,000, but less than \$25,000, may also be included in this series if automatic billing is desired. Calibration is not included in this series. Once the project has been established, the Finance Division automatically bills according to the terms of the agreement. Information on procedures is included in Subchapter 8.05. The projects in this series are grouped into the following two categories:

--570-574 State and Local Government and Nonprofit Organizations - This series includes work performed at the request of state and local governments. Also included are: (1) work for nonprofit associations and organizations engaged in a cooperative project with NIST as evidenced by the agreement (for example, NIST partially funds the work); (2) work and dissemination of the results of benefit to the public; and (3) work for an organization engaged in a nonprofit activity designed for the public safety, health, or welfare. The recovery of a use surcharge is required for work done in this series.

--575-579 Foreign Government and Public - This series includes work NIST does for foreign governments and public customers and requires the recovery of a use surcharge.

580-699 Expense and Income and Interdivision Services

Where the OU is establishing a project in the expense and income series for repeated performance of a similar activity for multiple sponsors, fees should be established in advance and submitted to the Budget Division for approval. Costs in projects in this series are billed to customers only on specific instructions to the Finance Division by the OU. For additional information on NIST policy and procedures on the fiscal operation of expense and income projects, refer to Subchapter 8.07 – Working Capital Fund.

The Expense and Income projects are grouped by the type of effort undertaken in the project.

--580-584 Seminars and Fee-Supported Conferences - These projects are established to record expenses and income derived from seminars and conferences which are sponsored, co-sponsored, or hosted by the National Institute of Standards and Technology. The projects are

managed at Gaithersburg and Boulder by the Public and Business Affairs Division. Income in the form of registration fees and co-sponsor contributions is collected by the Finance Division. Subchapter 14.06 outlines the process required for establishing these projects.

--585-594 Miscellaneous Services - These are projects established to accumulate expenses for travel and miscellaneous consultative and advisory services under \$25,000. Costs in these projects are to be billed to customers only on specific instructions furnished to the Finance Division by the OU. The projects in this series are grouped into the following two categories:

--585-590 *Federal Government* - This series includes projects established for the purpose of accumulating miscellaneous reimbursable consultative and advisory services, including travel, performed at the request of various federal agencies.

--591-594 *State, Local, and Foreign Government and Public* - Use surcharge applied - This series includes reimbursable consultative and advisory services, including travel, that NIST does for state, local, and foreign governments and public customers. The recovery of a use surcharge is required for work done in this series.

--595-599 Interdivision Services - See explanation below under MISCELLANEOUS.

--600-654 Calibration and Testing - The following is a guideline to assist in making the distinction between calibration and testing projects. If the intended use of a measurement value is to transfer that value to other instruments, then the effort can be classified as a calibration. If the measurement made is intended only to provide information about the subject unit, and there is no intent to use that information or value for measuring or comparing other instruments after the unit leaves the NIST laboratory, then the work can be classified as a test. Destructive product testing or acceptance testing would fall into this category. In the final analysis, the determination rests on the judgment of the technical OU. Questions concerning a particular item should be directed to the Calibration Program.

Explanations of additional terms are offered here.

Predetermined Fees - These fees are charged for a specific type of calibration or test and are published in special publications such as SP 250, NIST Calibration Services Users Guide. The fees are predetermined in an effort to spread the cost of a calibration evenly to all customers even though the cost factors may vary slightly from unit to unit during the year. Generally, these calibrations are low in dollar cost and adequate experience exists to set a uniform price.

Predetermined fees published in SP 250 must be charged to all customers receiving the calibration service. The use surcharge is included in the calculation, and no distinction is made as to whether the customer is a government agency or is non-government. In cases where the cost of performing an at-cost or special calibration is considered to be an extension of a schedule calibration, the published fee modified by some fixed ratio known to be valid for such operations may be charged under this series. The resulting fee is actually a modified predetermined fee. For example, if a published calibration calls for the calibration at ten points or values on the item and the customer wants calibrations at fifteen points, it would be possible to charge based on the

rate for ten points plus a factor for the additional effort. See Subchapter 8.07 Working Capital Fund for additional information on surcharges to be included in predetermined fees.

At-Cost Items - These are calibrations and tests of an unusual nature. They can be modifications of published items or involve a special job for which it is impractical to publish a predetermined fee. The calculation of the fee would be on an actual cost basis plus any applicable surcharges. Work done for state, local, and foreign governments and the public is subject to the use surcharge.

--600-629 Calibrations - Public and Government -- Use surcharge applied - These projects handle most of the calibration work outlined in SP 250. OU costs are billed based on Form NIST-64, Test Record, which is submitted directly to the Finance Division with a copy to the Calibration Program.

--630-644 Testing - State, Local, and Foreign Government and Public -- Use surcharge applied - These projects are for tests performed for state, local, and foreign governments and public sponsors. The costs in these projects are to be billed directly through the Finance Division by use of Form NIST-94, Statement of Services Performed by NIST, submitted by the OU. The OU should keep on file any necessary data as to number of tests and type. OUs that wish to set up a separate project to allow them to receive an order over \$5,000 and to have the Finance Division automatically bill the cost against the assigned financing should establish a project in the appropriate non-federal sponsors number series (570-579).

--645-654 Testing - Federal Government - These projects are for tests performed for various federal government agencies. The costs in these projects are billed directly by the Finance Division through use of Form NIST-94, Statement of Services Performed by NIST, submitted by the OU. The OU should keep on file any necessary data as to number of tests and type. OUs that wish to establish a separate project to allow them to receive an order over \$5,000 and to have the Finance Division automatically bill the cost against the assigned financing should establish a project in the federal sponsors number series (370-569).

--655-674 Standard Reference Materials Program-Surcharge Supported Activities - The projects in this series are established to record expenses incurred and income earned as defined below. Income to offset operations and service development support costs is generated by surcharges identified as part of the purchase price of each SRM sold. The SRM surcharges are computed annually by the Standard Reference Materials Program (SRMP) and are subject to approval by the Budget Division. The income appears in SRM sales projects. See Subchapter 8.07 Working Capital Fund for additional information.

--655-660 SRM Program Operations -- Projects in this series are established to record expenses incurred in the operation and administration of the Standard Reference Materials Program.

--661-665 SRM Sales - See explanation below under MISCELLANEOUS.

--666-674 SRM Service Development Support - Projects in this series are for research and development costs associated with specific SRMs in the pre-production stage.

675-679 Proprietary Measurements - Use surcharge applied

This series is for costs incurred in allowing use of specific measurement and test facilities by private parties who wish the resulting information to be treated as proprietary. The titles of projects in this series must identify the work as proprietary, the designated facility to be used, and the name of the concern doing the research.

680-684 Calibration Program Surcharge-Supported Activities

The projects in this series are established to record costs as defined below. Income to offset these costs is generated by surcharges identified as part of the purchase price of each calibration. The Calibration Program Operations Surcharge and the Service Development Support Surcharge are computed annually by the Calibration Program, subject to approval by the Budget Division. The income appears in the calibration surcharge supported projects in the Calibration Program. See Subchapter 8.07 Working Capital Fund for additional information.

--680 Calibration Program Operations - Projects in this series are established to record expenses incurred in the operation and administration of the Calibration Program.

--681-684 Calibration Service Development Support - Projects in this series are assigned by the Calibration Program to OUs to record costs associated with the development or improvement of specific calibration services.

685-699 Seminars and Fee-Supported Conferences

--685-699 Seminars and Fee-Supported Conferences - These Projects are established to record expenses and income derived from seminars and conferences which are sponsored, co-sponsored, or hosted by the National Institute of Standards and Technology. The projects are managed at Gaithersburg and Boulder by the Public and Business Affairs Division. Income in the form of registration fees and co-sponsor contributions is collected by the Finance Division. Subchapter 14.06 outlines the process required for establishing these projects.

700-799 Standard Reference Materials - Production

This series is used for projects established for the production of Standard Reference Materials (SRMs) to keep track of the investment of the Working Capital Funds authorized by the NIST Director for SRM production. When the production of materials is completed they are transferred to inventory. Costs are recovered as the SRMs are sold. (See Subchapter 8.07.)

Equipment

800-849 Working Capital Fund Invested Equipment (IE)

This series is used for equipment acquired as an investment of the Working Capital Fund. The Fund is reimbursed for the equipment cost through amortization charges that are based on a fixed payment determined by the organization and approved by the Budget Division. The equipment

may be purchased or may be manufactured within NIST. Information on the management of Working Capital Funds allocated for the purchase of invested equipment is included in Subchapter 8.11.

--800-809 Direct Purchase of WCF Invested Equipment

--810-849 Manufacture of WCF Invested Equipment

Institutional Support

900-919 Laboratory and Division Overheads

This series is set aside for use by laboratories or laboratory-level offices for the accumulation of organizational management, invested equipment loan repayment, and other appropriate indirect costs which are distributed on a pro rata basis to all sources of funding throughout the OU (except NIST Institutional Support) through the use of predetermined rates based on labor and personnel benefits charged.

--900-909 Division Overhead - Equipment Loan Repayment - Projects in this series collect only equipment loan repayment and surcharge costs.

--910-919 Laboratory Overhead - Projects in this series may collect labor, other objects, and equipment loan repayment and surcharge costs.

950-990 Institutional Support

This project series is used for activities, generally of a NIST-wide nature, approved for overhead funding by the Director. Institute overhead costs are recovered in three ways: (1) Projects in all other number series (including Laboratory Overhead) are assessed a predetermined percentage rate based on labor and personnel benefits charged; (2) charges are made to outside organizations which utilize NIST space or use other NIST overhead services; and (3) a contract/grant surcharge is assessed based on charges in grant and specified other services object classes. Assessment techniques for institutional support and management of institutional support projects are contained in Subchapter 8.07.

--950-974 Controllable Base

--975-978 Controllable Nonbase, from OU Reserve

--979 Controllable Nonbase, from NIST Director's Reserve

--980-989 Uncontrollable

--990 Special agency-wide Institutional Support Activities

Miscellaneous

595-599 Interdivision Services

The projects in this series include services performed by one OU and available to other OUs within NIST. (Interdivision services include computer services, photo and graphic arts, Fabrication Technology, Plant, etc.). Costs are accumulated in projects in this series and then transferred by appropriate object class to the benefiting organization. See Subchapter 8.08 for a description of how these services are charged to projects.

661-665 SRM Sales

Income resulting from SRM sales to the private sector, government agencies, and OUs within NIST is collected in these projects.

920-939 Storeroom Inventories

Working Capital Fund levels approved for investment in inventories are controlled through projects in this series. (See also Subchapter 8.07.)

940-949 Miscellaneous and Deputy Chief Financial Officer Use and 991-999

These series represent memorandum accounts for the purpose of balancing and monitoring budgetary and accounting records.

APPENDIX C

NIST BUDGET/PROGRAM STRUCTURE

301 Strategic and Engineering Research Initiatives

31 310 Electronics and Electrical Engineering

32 320 Manufacturing Engineering

33 330 Chemical Science and Technology

34 340 Physics

35 350 Materials Science and Engineering

36 Building and Fire Research

361 *Building Research

362 *Fire Research

37 370 Computer Science and Applied Mathematics

381 – NIST Center for Neutron Research

382 – Center for Nanoscale Science and Technology

39 Technology Assistance

391 *Technology Support

392 *Standard Reference Data

393 *Standard Reference Materials

394 *National Voluntary Laboratory

Accreditation Program

395 *Calibrations

401 Technical Competence Program

402 Postdoctoral Fellowship Program

403 Computer Support

407 Technical Reimbursable Services

408 Business Systems

41 410 National Quality Program

*Resource estimates at this level of detail are not separately identified in NIST budget submissions.

ACTIVITY/SUBACTIVITY PROGRAM CODES

5 Extramural Programs

510/511 Advanced Technology Program

510 *Advanced Technology Program - Intramural

511 *Advanced Technology Program – Extramural/Administration

512 – Technology Innovation Program

512 512 Manufacturing Extension Partnership

7 Construction and Major Renovations

71 Construction and Major Renovations

711 Construction and Major Renovations

712 Modifications and Improvements

713 External Projects

INSTITUTIONAL SUPPORT SUPPORTED ACTIVITIES

Office of the Director, NIST

610 Management Activities

612 Quality Programs

613 Civil Rights

614 Boulder Management Activities

616 Program Activities

619 International and Academic Affairs

Technology Services

630 Research and Technology Applications

631 Information Resources and Services Activities

Director for Administration and Chief Financial Officer

640 Management Activities

641 Management and Organization Activities

642 Human Resources Management Activities

643 Public and Business Affairs Activities

644 Gaithersburg Plant Activities

645 Facilities Services Activities

646 Occupational Health and Safety Activities

647 Acquisition and Assistance Activities

649 Boulder Engineering, Maintenance, Safety, and Support Activities

*Resource estimates at this level of detail are not separately identified in NIST budget submissions.

650 Financial Management Activities

651 Budget Activities

652 Finance Activities

653 Financial Systems Activities

654 DoC Assessments

Information Technology Laboratory

660 Computer Planning and Management

661 Information Systems

662 Telecommunications

Manufacturing Engineering Laboratory

670 Fabrication Technology Activities

APPENDIX D

NATIONAL SCIENCE FOUNDATION AND FIELD OF SCIENCE CODES

Each year NIST must submit to the National Science Foundation (NSF) a detailed report concerning federal scientific activities. This information on federal investment in science and technology is increasingly sought and used by the executive and legislative branches of the federal government for policy and management purposes as well as by industrial and academic groups. To provide up-to-date information on research and development (R&D) activities, cost centers must be coded according to the coding scheme provided in Section 1 of this Appendix.

The NSF also requires information on fields of science. For NIST to provide this information, cost centers must be coded according to the coding scheme provided in Section 2 of this Appendix.

(1) The following NSF codes are to be used:

Research and Development

--Basic Research - code 1

--Applied Research - code 2

--Development - code 3

Non-R&D - code 4

Research and development include all direct, indirect, incidental, or related costs resulting from or necessary to the performance of research and development as defined below regardless of whether the research and development are performed by a federal agency (intramural) or by private individuals and organizations under grant or contract (extramural). Research and development exclude routine product testing, quality control, mapping and surveys, collection of general-purpose statistics, experimental production, and activities concerned primarily with the dissemination of scientific information and the training of scientific staff.

NSF Code Definitions

Research is systematic, intensive study directed toward fuller scientific knowledge of the subject studied. Demonstration activities that are intended to prove or to test whether a technology or method does, in fact, work are included in the definition of research and development.

--Basic Research - is concerned primarily with gaining a fuller knowledge or understanding of the subject under study without specific applications toward processes or products in mind.

--Applied Research - is primarily interested in a practical use of knowledge or understanding for the purpose of meeting a recognized need.

Development - is systematic use of the knowledge and understanding gained from research directed toward the production of useful materials, devices, systems, or methods, including design and development of prototypes and processes. It excludes quality control, routine product testing, and production.

Non-R&D - includes technical services which are not covered by the definitions for Research or Development.

(2) The following Field of Science codes are to be used. Terms in brackets have been added by NIST.

a. Physical sciences are concerned with the understanding of the material universe and its phenomena. They comprise the fields of astronomy, chemistry, physics, and physical sciences not elsewhere classified. Examples of disciplines under each of these fields are as follows:

11 - Astronomy: laboratory astrophysics; optical astronomy; radio astronomy; theoretical astrophysics; X-ray, Gamma-ray, and neutrino astronomy

12 - Chemistry: analytical; inorganic; organo-metallic; organic; pharmaceutical; physical; polymer sciences (except biochemistry)

13 - Physics: acoustics; atomic and molecular; condensed matter; elementary particles; nuclear structure; optics; plasma; solid state; theoretical/mathematical

19 - Physical sciences, n.e.c.*

b. Mathematics and computer sciences employ logical reasoning with the aid of symbols and are concerned with the development of methods of operation employing such symbols, and in the case of computer sciences, with the application of such methods to automated information systems. Examples of disciplines under these fields are as follows:

21 - Mathematics: algebra; analysis; applied mathematics; foundations and logic; geometry; numerical analysis; statistics; topology; operations research

22 - Computer sciences: computer and information sciences (general); design, development, and application of computer capabilities to data storage and manipulation; information sciences and systems; management information systems; programming languages; systems analysis

29 - Mathematics and computer sciences, n.e.c.*

c. Environmental sciences (terrestrial and extraterrestrial) are concerned with the gross nonbiological properties (with one exception) of the areas of the solar system that directly or indirectly affect human survival and welfare; they comprise the fields of atmospheric sciences, earth sciences, oceanography, and environmental sciences not elsewhere classified. The one exception is that obligations for studies pertaining to life in the sea or other bodies of water are to

be reported as support of oceanography and not biology. Examples of disciplines under each of these fields are as follows:

31 - Atmospheric sciences: aeronomy; air pollution; extraterrestrial atmospheres; metrology; solar; weather modification

32 - Earth sciences: engineering geophysics; general geology; geodesy and gravity; geomagnetism; hydrology; inorganic geochemistry; isotopic geochemistry; organic geochemistry; laboratory geophysics; paleomagnetism; paleontology; physical geography; seismology sciences

33 - Oceanography: biological oceanography; chemical oceanography; physical oceanography; marine/aquatic biology

39 - Environmental sciences, n.e.c.*

d. Engineering is concerned with studies directed toward developing engineering principles or toward making specific scientific principles usable in engineering practice. Engineering is divided into eight fields: aeronautical, astronautical, chemical, civil, electrical, mechanical, metallurgy and materials, and engineering not elsewhere classified. Examples of disciplines under each of these fields are as follows:

41 - Aeronautical: aerodynamics

42 - Astronautical: aerospace; space technology

43 - Chemical: chemical engineering; petroleum engineering; petroleum refining process; polymer/plastics engineering; wood science

44 - Civil: architectural; environmental/environmental health engineering; geotechnical; hydraulic; hydrologic; sanitary and environmental; structural; transportation

45 - Electrical: computer engineering; electrical, electronics, and communications engineering; power engineering

46 - Mechanical: engineering mechanics; mechanical engineering

47 - Metallurgy and materials: ceramic sciences and engineering; geological engineering; geophysical engineering; materials engineering; materials research; materials science; metallurgical engineering; metallurgy; mining and mineral engineering; textile sciences and engineering; welding

49 - Engineering, n.e.c.* agricultural engineering; bioengineering and biomedical engineering; engineering design; engineering physics; engineering science; general engineering; industrial/manufacturing engineering; nuclear engineering; systems engineering; systems science and theory; other engineering

80 [Cryogenics] - cryoelectronics; cryogenic materials; refrigerants; superconductors; temperature standards

81 [Measurement] - research related to standards, calibrations, or testing; this field to be used only if engineering fields above cannot be used

82 [Other]

e. Life sciences are concerned with the study of living organisms and their systems. It consists of five detailed fields: biological (excluding environmental), environmental biology, agricultural, medical, and life sciences not elsewhere classified. The illustrative disciplines provided below under each of these detailed fields are intended to be guidelines, not sharp definitions; they represent examples of disciplines generally classified under each detailed field. A discipline, however, may be classified under another detailed field when the major emphasis is elsewhere. Research in biochemistry could be reported as biological, agricultural, or medical, depending on the orientation of the project. Human biochemistry would be classified under biological, but animal biochemistry or plant biochemistry relating to food production would be under agricultural. In no case should the research be reported under more than one field. No double counting is intended or allowed.

51 - Biological

(excluding environmental): anatomy; biochemistry; biology; biometrics and biostatistics; biophysics, biotechnology; botany; cell biology; ecology; entomology and parasitology; epidemiology; genetics; microbiology; neuroscience (biological); nutrition; pathology; physiology; toxicology; virology; zoology; other biological, n.e.c.*

54 - Environmental biology: biotic community ecology; ecosystem sciences; evolutionary biology; global warming; limnology; population biology; systematics; other environmental biology, n.e.c.*

55 - Agricultural sciences: agronomy; animal sciences; conservation; agriculture chemistry; fish and wildlife; forestry; horticulture; plant sciences; soil science; phytoproduction; agriculture, general; other agriculture, n.e.c.*

56 - Medical sciences: anesthesiology; cardiology; dentistry; dermatology; gastroenterology; geriatrics; hematology; neurology; neuroscience; nuclear medicine; obstetrics and gynecology; oncology; ophthalmology; optometry; orthopedics; osteopathic medicine; otorhinolaryngology; pediatrics; pharmacology; podiatry; preventive medicine; psychiatry; public health; radiobiology; radiology; surgery; urology; other medical basic sciences; n.e.c.*

59 - Life sciences, n.e.c.* administrative services; allied health; communication disorders; gerontology; health professions and related services; medical laboratory sciences and services; multidisciplinary projects within life sciences; nursing technologies; occupational therapy; physical therapy; rehabilitation/therapeutic services

f. Psychology deals with behavior, mental processes, and individual and group characteristics

and abilities. Psychology is divided into three categories: biological aspects, social aspects, and psychological sciences not elsewhere classified. Fields are as follows:

61 - Biological aspects: animal behavior; clinical psychology; comparative psychology; ethology; experimental psychology; psychometrics

62 - Social aspects: child psychology; development and personality; development psychology; educational, school, vocational psychology; industrial and engineering psychology; social psychology

69 - Psychology, n.e.c.*

g. Social sciences are directed toward an understanding of the behavior of social institutions and groups and of individuals as members of a group. Social sciences include anthropology, economics, political science, sociology, and social sciences not elsewhere classified. Examples of disciplines under the field of social sciences are as follows:

71 - Anthropology: applied anthropology; archaeology; cultural and personality anthropology; ethnology; social anthropology

72 - Economics: Agricultural economics, applied economics; business/managerial economics; econometrics; industrial economics; international economics; labor economics; public finance and fiscal policy; quantitative economics; resource economics

74 - Linguistics: anthropological/archaeological linguistics; computational linguistics; psycholinguistics; sociolinguistics

75 - Political science: area or regional studies; comparative government; international relations and affairs; legal systems; political science and government; political theory; public administration; public policy analysis

76 - Sociology: city, community, and regional planning; comparative and historical; complex organizations; criminology; culture and social structure; demography; ethnic studies; group interactions; social problem and welfare theory; sociology; urban studies/affairs

79 - Social sciences, n.e.c.*: socioeconomic geography; research in law and science; geography; general social sciences

h. 99 - Other sciences n.e.c.*: Used when the multidisciplinary and interdisciplinary aspects make classification under one primary field impossible.

i. 00 - Non - R&D

*Not elsewhere classified. To be used for multidisciplinary projects within the broad field and for single-discipline projects for which a separate field has not been assigned.

BUDGET FORMULATION

Sections

8.03.01 Purpose

8.03.02 Scope

8.03.03 Policy

8.03.04 Definitions

8.03.05 Budget Formulation Cycle

8.03.06 Responsibilities

8.03.07 References

8.03.01

PURPOSE

This subchapter provides information on the formulation aspects of the appropriation process and describes the responsibilities for preparation and justification of NIST budget requests.

8.03.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

8.03.03

POLICY

It is NIST policy to prepare and justify its budget submissions for appropriated funds in accordance with guidelines provided by the Congress, the Office of Management and Budget (OMB), and the Department of Commerce.

8.03.04

DEFINITIONS

a. Appropriation - Enacted legislation providing authority to incur obligations and to make payments out of the Treasury for specified purposes during a specified period of time. An appropriation is the most common means of providing the budget authority needed to incur obligations for expenses which are necessary for or incident to the proper execution of the purpose, unless the expenses are otherwise prohibited.

b. Authorizing Legislation - An act of Congress that establishes or continues a federal program or agency either for a specified period of time or indefinitely; specifies its general goals and conduct; and may suggest a level of budget authority needed to fund the program or agency, which is subsequently provided in a future appropriation act. An authorization for an agency or

program usually is required before an appropriation for that same agency or program can be passed.

c. Budget - A plan for the use of resources to accomplish goals and objectives.

d. Budget Amendment - A revision to a pending budget request, submitted to Congress by the President before Congress completes appropriations action.

e. Budget Formulation - All steps, actions, and informational output of the budget process which are required in advance of the enactment of an appropriation bill by Congress. It is the process by which the resources necessary to accomplish NIST goals and objectives are determined and justified to decision-makers (the Secretary, the President, and the Congress).

f. Budget Justification - A narrative and tabular description of goals, objectives, performance measures, and representative accomplishments and the costs of achieving them.

g. Budget Supplemental - An additional amount requested for appropriation for the current year after enactment of the regular appropriation. The request should be for needs deemed too urgent to be postponed until enactment of the next regular appropriation.

h. Continuing Resolution - A joint resolution enacted by Congress usually at the beginning of the fiscal year to provide authority and necessary funding for federal agencies and programs to continue operations until the regular fiscal year appropriation is enacted. The continuing resolution usually specifies a maximum rate at which the agency may incur obligations.

8.03.05

BUDGET FORMULATION CYCLE

a. The objective of the formulation process is to provide a satisfactory information basis upon which Bureau directors, Agency heads, the President, and Congress can make knowledgeable decisions in the allocation of the resources toward fulfillment of the Nation's goals and needs.

b. The basic framework of budget formulation in the federal government is established by law. OMB and departmental guidance provide specific details. The primary elements in this framework are:

-- Authorization - The Congress must authorize the obligation of funds for specific programs as a prerequisite for subsequent appropriation. Authorization bills may be submitted by Department heads with the approval of OMB, submitted by the President, or initiated by Congress. Congressional review of programs for the authorization of appropriations occurs at hearings held by the standing legislative committees of the House and Senate.

-- Budget Requests - NIST submits detailed budget request documents to the Secretary. After review by the Department and based on the decisions of the Secretary, bureaus prepare revised budget requests for submission to OMB. Decisions at this level form the basis for the annual congressional budget, which is submitted by the President to Congress by the first Monday in February. NIST prepares and submits justifications providing additional detailed information.

Budget amendments or supplemental requests may be submitted to Congress by the President under certain conditions.

-- Appropriation - Appropriations subcommittees in both the House and Senate hold hearings to consider the President's budget. Recommendations are presented to the full committees and to the full House and Senate. A conference committee resolves differences in the House and Senate versions of the appropriations bill. Upon acceptance of conference action by both the House and the Senate, the appropriations bill is sent to the President for signature. The President can approve or veto the bill. When an appropriations bill has not been enacted by the beginning of the fiscal year for which the funds are requested, Congress enacts a temporary appropriation act or "continuing resolution," which authorizes the agency to continue its operations for a designated time period. Subsequent continuing resolutions may be passed to continue operations until an appropriation bill is enacted.

c. Also included in budget formulation are the planning, study, evaluation, review, and decision-making actions which must be taken at the bureau and the departmental levels which are necessarily precedent to and supportive of the elements described above.

d. The nature and amounts under consideration in the budget are confidential and will not be released outside of the Administration until the budget is transmitted formally to Congress by the President.

8.03.06

RESPONSIBILITIES

a. Planning and Program Review - The Program Office and the Budget Division are responsible for establishing procedures, guidelines, and schedules for the planning and program review process. The Program Office and the Budget Division provide advice to NIST management on funding levels and program content.

As part of ongoing, internal planning and program review, organizational units are responsible for presenting programs and proposed budget initiatives for review by NIST management officials.

The Director determines the content of the proposed NIST budget in accordance with administrative guidelines on the preparation and submission of the budget.

b. Budget Authorization - The Program Office and the Budget Division cooperate with the Office of Congressional and Legislative Affairs in the preparation of material for the Congressional authorization process.

c. Budget Justification - The Budget Division is responsible for coordinating the preparation of the required budget justifications to DoC, OMB, and the Congress. The Public and Business Affairs Office coordinates with the Budget Division in preparing information for release to the public.

d. Legislative Proposals - The Budget Division works closely with the Congressional and

Legislative Affairs Office to draft amendments and legislative proposals which are submitted through the Department of Commerce for consideration at the next session of Congress.

8.03.07

REFERENCES

The following provisions of pertinent statutes and OMB and DoC guidance relate to budget formulation:

-- United States Code Title 31, Subtitle II, Chapter 11, -- "The Budget and Fiscal, Budget, and Program Information" - accessible at:
http://www.access.gpo.gov/uscode/title31/subtitleii_chapter11_.html

-- United States Code Title 31, Subtitle II, Chapter 13 -- "Appropriations" -- accessible at:
http://www.access.gpo.gov/uscode/title31/subtitleii_chapter13_.html

-- Office of Management and Budget Circular No. A-11 -- "Preparation and Submission of Budget Estimates" -- accessible at: <http://www.whitehouse.gov/omb/circulars/index.html>

-- Department Administrative Order 203-1 -- "Appropriation Requests and Related Budget Matters" -- accessible at: <http://dms.osec.doc.gov/cgi-bin/doit.cgi?218:112:1:2>

-- Department of Commerce "Budget and Program Analysis Handbook" -- accessible at:
<http://www.osec.doc.gov/bmi/budget/Budget%20Handbook.htm>

Subchapter 8.04 Appropriated Funds

Sections

8.04.01 Purpose
8.04.02 Scope
8.04.03 Policy
8.04.04 Responsibilities
8.04.05 Definitions
8.04.06 Apportionments and Reapportionments
8.04.07 Allocations to Operating Units
8.04.08 Operating Budgets
8.04.09 Funds Control and Reporting
8.04.10 Reprogramming
8.04.11 Disposition of End-of-Year Unobligated Balances and Over- and Under-Accrual of Prior Year Obligations
8.04.12 Review and Evaluation
8.04.13 References
Appendix A - Requirements Under the Antideficiency Act

8.04.01

PURPOSE

This subchapter discusses the management and control of appropriated funding.

8.04.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

8.04.03

POLICY

Obligations of appropriations are to be restricted to the amounts apportioned by OMB. In addition: (1) all representations in the budget transmittal by the President, in the estimates and justifications submitted by the Department, and in testimony of departmental witnesses shall be adhered to; and (2) all expressions of Congressional intent stated in committee reports or in discussion on the floor of the Congress with respect to the objects or purposes for which funds are appropriated shall be adhered to, unless the Secretary specifically authorizes or directs a different course of action or unless a notification of reprogramming has been transmitted to the Congress.

8.04.04

RESPONSIBILITIES

a. The Director is responsible for administrative control of NIST appropriated funds. This includes:

(1) Developing financial management systems and procedures consistent with the requirements of the DoC Budget and Program Analysis Handbook and Accounting Principles and Standards Handbook;

(2) Allocating funds to heads of Operating Units (OUs);

Effective Date: 9/8/06

Subchapter 8.04 Appropriated Funds

(3) Ensuring that operations are maintained within the limits of approved apportionments, financial plans, and operating budgets; and

(4) Providing notification to appropriations committees and obtaining proper clearances prior to proceeding with reprogramming actions.

b. The Chief Financial Officer (CFO), in cooperation with the Budget Officer and the Chiefs of the Finance Division and Business Systems Division, is responsible for developing procedures to provide financial and employment data needed for administrative control and reporting requirements and for maintaining liaison with the DoC Office of Budget and the Office of Financial Management on resolution of problems.

(1) Specific responsibilities of the Budget Officer are as follows:

(a) Preparation of apportionment and reapportionment requests and backup, and periodic reports and other required data;

(b) Allocation of budgetary resources to OUs in support of the programmatic distribution of funds appropriated by Congress, quarterly apportionments approved by OMB, and decisions by the NIST Director;

(c) Issuance of operating budgets to OUs and divisions reflecting the programmatic distribution of funds appropriated by Congress; and

(d) Clearance and/or preparation and release of financial data from official records in response to miscellaneous external requests for information.

(2) Specific responsibilities of the Chief of the Finance Division are as follows:

(a) Organizing, planning, developing, coordinating, and managing a comprehensive accounting/finance program for NIST; and

(b) Certifying the accuracy of official accounting records and reports.

(3) The Business Systems Division is responsible for maintaining a financial management system that produces reports which show accrued costs, total obligations, unobligated balances, and total budgetary resources available to NIST.

c. OU Directors are responsible for establishing division operating levels and project authorizations and ensuring that operations are maintained within limits of allocations issued by the Budget Division.

Subchapter 8.04

Appropriated Funds

d. Specific responsibilities regarding operating budgets and administrative control of funds are given in Appendix A.

8.04.05

DEFINITIONS

a. Allocation - At NIST, approval by the Director for OU Directors to incur obligations up to a set level of funding. The sum total of allocations must equal the apportionment. Suballocations or operating levels to division chiefs are established by the OU Directors consistent with the programmatic distribution of funds appropriated by the Congress and quarterly apportionments approved by OMB.

b. Allotment - An administrative subdivision of appropriated funds below the apportionment level. Allotments are used by the head of an agency to delegate to agency employees authority to incur obligations within a specified amount pursuant to an OMB apportionment or other statutory authority.

c. Antideficiency Act - Refers to 31 U.S.C. 1341 and related sections, which make it a violation of law for an agency to incur obligations or make expenditures in excess of an appropriation or apportionment or in advance of an appropriation.

d. Apportionment - A distribution made by OMB of amounts available for obligation in an appropriation or fund account into amounts available for specified time periods, programs, activities and/or objects. The amounts so apportioned limit the obligations that may be incurred.

e. Appropriation - Enacted legislation providing authority to incur obligations and to make payments out of the Treasury for specified purposes during a specified period of time. See Subchapter 8.03, Budget Formulation.

f. Budget Authority - Authority provided by law which permits government agencies to enter into financial obligations requiring either immediate or future cash disbursements.

g. Deferral - An action or inaction that temporarily withholds, delays, or precludes the obligation or expenditure of budget authority. Deferrals may only be for the purposes authorized by the Antideficiency Act and may not be made for policy reasons. They may not extend beyond the end of the fiscal year in which the funds are withheld. The President must advise Congress of proposed deferrals, and either House of Congress may overturn a deferral by passage of an impoundment resolution.

h. Full-Time Equivalent (FTE) - Total number of hours paid or to be paid in the reporting year divided by 2080. It is always 2080 hours, even in fiscal years with extra compensable days.

i. Impoundment - Any action or inaction by the President or a federal agency that delays or withholds the obligation or expenditure of budget authority provided by the Congress. There are two categories of impoundments: deferrals and rescissions.

Subchapter 8.04

Appropriated Funds

- j. Obligation – A binding agreement (amount of an order placed, contract awarded, service received, or similar transaction) that will result in cash disbursements, either immediately or in the future.
- k. Operating Budget - Allocation of appropriated funds by budget/program code which is issued by the Budget Division to heads of OUs and division chiefs.
- l. Outlays, Net - Gross payments made to liquidate obligations incurred (cash payments or issuance of checks) less reimbursements, refunds, and loan repayments received and credited in the appropriation or fund accounts; the net of disbursements less receipts.
- m. Program Code - Coding number assigned to each project to identify the budget activity, subactivity, line item, and program under which the project is identified (also referred to as budget/program code).
- n. Program Manager - Individual assigned responsibility for developing and presenting program objectives and plans and monitoring technical and fiscal progress for a particular NIST-wide program.
- o. Program, Project, or Activity (PPA) - major area of work for which funding is identified in the budget submission (budget subactivities and line items) to Congress or as provided in the enacted appropriations bill or committee reports accompanying the appropriations bill.
- p. Reapportionment - A revision by OMB of a previous apportionment.
- q. Reclassification - Any change in the project budget/program code designation not involving a change in program objectives.
- r. Reprogramming - The shifting of resources within an appropriation account from one PPA to another to use them for purposes other than those outlined in the budget justifications or expressed as Congressional intent in the enacted appropriations bill and committee reports.
- s. Rescission - A Presidential request that Congress cancel (rescind) all or part of an appropriation or available unobligated balances. Generally, amounts proposed for rescission are withheld for up to 45 calendar days of continuous session while the Congress considers the proposals. Unless both Houses of the Congress complete action on a rescission bill within that time period, the budget authority must be made available for obligation. Congress may also initiate rescissions through its own appropriations process. Such action occurs for various reasons, including changing priorities, program terminations, excessive unobligated balances, and program slippage.
- t. Reserve - Portions of appropriations, funds, or contract authority set aside for contingencies or savings. Reserves established by OMB on an apportionment can only be

Subchapter 8.04

Appropriated Funds

released by means of an approved reapportionment. Such reserves must be reported to the Congress under the provisions of the Impoundment Control Act of 1974.

u. Working Capital Fund - The NIST revolving fund established by Congress in 1950 (see Subchapter 8.07).

8.04.06

APPORTIONMENTS AND REAPPORTIONMENTS

a. 31 U.S.C. 1512 requires that all appropriations be administratively apportioned: (1) to ensure their obligation at a controlled rate which will prevent deficiencies from arising before the end of the fiscal year; and (2) to ensure that there is no drastic curtailment of the activity for which the appropriation is made.

Appropriations are commonly apportioned by quarter, based on estimated obligations to be incurred each quarter. At the end of each quarter, unobligated balances of apportionment are available, on a cumulative basis, for obligation in subsequent quarters without reapportionment unless otherwise specified by OMB. Apportionments also may be in total by specific programs, projects, activities, objects, or combinations thereof. The NIST Working Capital Fund was exempted from the apportionment requirement by OMB in 1975.

b. Preparation and Submission of Schedules - Requests for apportionment of NIST appropriations are submitted to OMB through the Department on the Apportionment and Reapportionment Schedule, SF-132, by August 21 of each year or within ten days after approval of the appropriation act, whichever is later. Financial plans which are consistent with the subactivity levels presented in the budget are submitted in support of the schedules (see Section 8.04.09). The Budget Division is responsible for the preparation and submission of the schedules.

At OMB, apportionment requests are referred to the examiners responsible for the programs involved, who review requests and the supporting material to arrive at recommendations on amounts to be apportioned. OMB is required to act on the apportionment request by September 10, or within 30 days after the approval of the appropriation act, whichever is later.

A request for reapportionment is submitted as soon as a change in a previous apportionment becomes necessary due to a change in resources or within ten days after legislation is passed which changes budget authority.

c. Apportionment Reserves - Reserves may be established by OMB only to provide for contingencies, or to effect savings whenever savings are made possible by or through changes in requirements or greater efficiency of operations. Amounts reserved may not be obligated by the agency but may be released in whole or in part by reapportionment action by OMB at any time during the year or by Congressional action on proposed rescissions or deferrals. Reserves must be reported by the President to the Congress as either a proposed rescission or a proposed deferral. Proposed rescissions must be released if both Houses of Congress have not completed action on the rescission bill within 45

Subchapter 8.04

Appropriated Funds

days. Proposed deferrals must be released if either House of Congress passes an impoundment resolution disapproving such proposed deferral.

d. Apportionment Control - The original copy of an approved apportionment is maintained by the Budget Division. The Budget Division records the apportionment in the financial management system, Commerce Business System (CBS), in which funds are controlled at the appropriation level. The Budget Division ensures from its control records that quarterly OU allocations are within the apportioned amounts. The Finance Division verifies that obligated balances in the standard general ledger accounts do not exceed apportioned amounts.

e. Employment and Outlay Ceilings - OMB may establish ceilings on employment and issue target outlay ceilings as supplements to the apportionment process. Although special requirements are imposed by law from time to time, generally OMB ceilings are applicable as administrative rather than legal limitations, and they are issued on an agency-wide basis rather than on an individual appropriation basis.

8.04.07

ALLOCATIONS TO OPERATING UNITS

a. Through the Budget Division, the Director assigns total allocations of appropriations, with quarterly breakdowns by program code, to the OU Directors. The sum of the allocations may not exceed the quarterly distribution and total appropriation amounts, in accordance with the provisions of the Antideficiency Act. These allocations constitute authority for OU Directors to incur obligations or costs within a given amount.

The OU Directors divide their allocations by assigning operating levels to division chiefs within their OU. In addition, managers of NIST-wide programs provide operating levels to all organizational units which receive program funding. These operating levels are further divided into project authorizations by quarter, which are entered into CBS.

The initial allocation is intended to provide for the performance of the primary responsibilities of the OU throughout the fiscal year. The OU Director is responsible for conducting the program within the limits of the allocation. In the event that an allocation is exceeded, the OU Director or division chief directly responsible for the overrun may be subject to administrative discipline if the circumstances warrant. The statutory penalties of the Antideficiency Act concerning over-obligation of funds do not apply to the allocations to the OU Director, except as they affect NIST as a whole. However, it is important that each OU Director recognize their responsibility to conduct operations within the allocation.

b. The Budget Division issues revised OU quarterly allocations to reflect changes due to transfer of funds, distribution of unobligated balances, distribution of additional appropriations, rescission of funds, and other financing adjustments. The Budget Division should be informed as soon as possible if it appears that a departure from the quarterly plan is necessary. A reapportionment may be obtained if the change cannot be

Subchapter 8.04 Appropriated Funds

accommodated within the existing apportionment.

8.04.08

OPERATING BUDGETS

a. Development of Annual Operating Budgets - The base point for developing operating budgets for appropriated funds for the coming year is the budget as communicated to the Congress. During the spring of each year, the Budget Division develops for the Director's approval funding levels for each appropriation by program and OU. These levels are determined by the timing of Congressional action, but they normally are the House or Senate Allowance or the level of the previous fiscal year, whichever is lower. These funding levels are issued to OU Directors prior to the beginning of each fiscal year. OUs establish project authorizations by quarter that reflect estimated annual spending.

b. Issuance of Operating Budgets - The Budget Division issues operating budgets at OU and division levels at the start of the fiscal year. Each month, revised operating budgets are issued to reflect any changes in funding or program levels. OU operating budgets support the NIST financial plans throughout the year (see Section 8.04.09).

8.04.09

FUNDS CONTROL AND REPORTING

a. 31 U.S.C. 3512 specifies that agency heads are responsible for establishing and maintaining accounting and internal control systems that provide reliable accounting for agency activities that will be the basis for preparing and supporting the agency budget request and for executing the agency budget.

Reports generated from the financial management system reflecting financial status are used by NIST management to maintain obligations within authorized levels and to comply with any restrictions included in appropriations acts. Managers must reconcile any locally-maintained records to the official accounting records in CBS.

NIST-wide year-end analyses are performed to ensure that all transactions affecting the appropriation and fund balances have been recorded properly, accurately, completely, and on a timely basis. All estimated obligations are reviewed for reasonableness and appropriateness, and adjustments are made as necessary.

b. External Reporting Requirements - The OMB and DoC systems for control of funds require periodic reporting against approved plans to evaluate progress and detect early deviations from approved plans.

The Finance Division prepares a quarterly Report on Budget Execution, SF-133, and an annual Year End Closing Statement, FMS 2108, for each NIST appropriation or fund account that are submitted to Treasury via the Federal Agencies' Centralized Trial Balance System (FACTS II). The Budget Division reviews the SF-133s and advises the Finance Division of their concurrence prior to transmittal. Certified copies are also provided to the DoC Office of Financial Management and DoC Office of Budget.

The Budget Division prepares the following for submission to the Department and OMB:

(1) Outlay plans by appropriation by month. Revisions to the initial plan and reports of actual outlays are required during the year.

Subchapter 8.04 Appropriated Funds

(2) Financial plans of obligations by appropriation by budget subactivity by month.

(3) Staffing plans showing FTE and onboard staffing estimates by month for NIST in total.

Revisions to the financial and staffing plans may be made to reflect changes in OMB ceilings, approved reprogramming, or changes which require reapportionment of funds. Reports against the financial and staffing plans are submitted monthly to DoC by the Budget Division. Variances of more than ten percent from the budget subactivity plan must be explained. Affected OU management and program managers will be asked to provide supporting information.

8.04.10

REPROGRAMMING

a. Reprogramming is the technical term applied to the transfer of funds and associated positions between programs, projects, or activities (budget subactivities or line items) which results in a change in the resources for a PPA from that reflected within the Congressionally approved budget for the current fiscal year. In addition, it includes:

(1) Proposals to use apportionment reserves or unobligated balances available from prior-year appropriations for purposes other than those for which they were appropriated; and

(2) Significant changes in program direction or output (without transfer of funds) from those justified in the budget.

b. As specified in the General Provisions of the annual Appropriations Act, proposed reprogramming actions which equal or exceed \$750,000 or ten percent of a PPA require Congressional approval. The Budget Division is responsible for submitting external notifications of reprogramming to DoC, OMB, and Congress in the required formats before the reprogramming is effected. Congress has 15 days to respond to a reprogramming notification.

c. OU Directors may propose a reprogramming action (both within and exceeding the NIST statutory limitations) for consideration by the Director. The request should be sent to the Director through the Budget Officer and must include a justification of the reprogramming and details of the resources involved.

8.04.11

DISPOSITION OF END-OF-YEAR UNOBLIGATED BALANCES AND OVER- AND UNDER-ACCRUAL OF PRIOR-YEAR OBLIGATIONS

a. All recorded obligations against NIST appropriations are financed from funds authorized by the Director. Until the obligations are liquidated (paid) or cancelled, these obligations and authorizations are carried forward and identified with the fiscal year of obligation. Since NIST appropriations are "no-year appropriations," which means that obligations may be incurred beyond the end of the fiscal year for which the appropriation

Subchapter 8.04

Appropriated Funds

was made, the following procedures have been established to ensure the effective and timely utilization of all funds, consistent with program plans.

b. End-of-Year Unobligated Balances - For the Scientific and Technical Research Services appropriation, each OU may retain for use in the following fiscal year unobligated balances of up to one-half of one percent of its total budgetary resources. An OU may request the Director's approval to retain additional balances when circumstances warrant (for example, a large increase which was not apportioned until too late in the year to be fully obligated). The justification in support of the request must be specific as to the programs, contracts, projects, and affected milestones for which carryover is needed. Specific instructions for such requests are issued by the Budget Division during the fourth quarter of the fiscal year.

Unobligated balances in the Construction of Research Facilities and Industrial Technology Services appropriations are authorized in total to the program managers, once they are apportioned by OMB.

c. Over- and Under-Accrual of Prior-Year Obligations - Unliquidated obligations do not always accrue for exactly the same amount as the original obligation. In the case of obligations that were made in prior years, this may result in unbilled costs, which must be covered, or may result in excess balances.

Changes in prior-year payments and obligations are monitored throughout the year by the Budget Division and the Finance Division. Generally, they are summarized by OU and program code at the end of the fiscal year, and balances will be added to carryover allocations or deficits will be netted against budgetary resources. If a particular organizational unit shows a pattern of consistent or large prior-year deficits, the transactions are reviewed and corrective action, if necessary, is recommended to NIST management.

In unusual circumstances, when a prior-year recovery becomes available and is needed during the current fiscal year, the OU may request by memorandum to the Budget Division that the balance be made available in the current fiscal year. The amount should be at least \$10,000, and the memorandum should supply sufficient justification as to (1) why the funds were deobligated and (2) why the funds are needed in the current fiscal year. The Budget Division may return the funds to the requesting division only if the apportionment will not be exceeded and if year-to-date OU and NIST recovery levels are sufficient to permit such an allocation.

8.04.12

REVIEW AND EVALUATION

a. Within the Department, the Office of the Inspector General and offices under the Chief Financial Officer have joint responsibilities for evaluating the program and financial performance of the bureaus and offices. The Office of the Inspector General conducts centralized management audits of the operating, administrative, and financial activities of

Subchapter 8.04

Appropriated Funds

all organizational units, and of selected claims, costs, cost proposals, and cost and pricing data arising from contracts, grants, subsidies, and loans or other similar agreements entered into or proposed by bureaus of the Department. The offices under the DoC CFO conduct program studies and analyses, prepare reports on program and fiscal status, and perform assessments of internal controls over reporting.

b. The Government Accountability Office (GAO) conducts independent audits of the operations of the Department. GAO serves as the chief administrative arm of the Congress to ensure that laws relating to program management and financial operations of the government are being properly observed. GAO reports directly to the Congress on its findings.

8.04.13

REFERENCES

Regulations governing management of appropriated funds include:

Title 31 of the United States Code (Money and Finance), specifically:

--Sections 1341-1342, 1349-1351, 1511-1519

--Sections 1101, 1104-1108, 3324

--Sections 1501-1502

2 U.S.C. 681-688 (Title X of P.L. 93-344, The Impoundment Control Act of 1974)

The following are the provisions of additional pertinent statutes and OMB and DoC guidance relating to management of appropriated funds.

a. 31 U.S.C. 1301 limits the purpose for which funds may be spent. It states that "Appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law."

b. The Antideficiency Act requires that all appropriations be apportioned to prevent obligations or expenditures in a manner which would necessitate deficiency appropriations, and requires a review by OMB at least four times a year of apportionments and reserves, including a determination as to whether reserves should be established, modified, or released [31 U.S.C. 1512]; provides that financial apportionments are made by the President (Director of OMB) [31 U.S.C. 1513(b)(1)]; and provides that obligations or expenditures are not to be incurred or authorized in excess of such apportionments or reapportionments [31 U.S.C. 1517(a)].

c. 31 U.S.C. 1108(b)(1) prescribes the use of cost-based budgets in administrative subdivision of appropriations and funds and their use in administration and operation.

d. 31 U.S.C. 1501(a) sets forth the legal definition of an obligation and provides that no amount be recorded as an obligation unless it is supported by documentary evidence.

e. 31 U.S.C. 1112(e) requires consistency in accounting and budget classifications, synchronization between such classifications and organizational structure, and support of budget justifications by information on performance and program costs.

Subchapter 8.04

Appropriated Funds

- f. Federal Managers' Financial Integrity Act (FMFIA) of 1982 provides the statutory basis for management's responsibility for and assessment of internal financial controls.
- g. OMB Circular A-11, Preparation, Submission, and Execution of the Budget, provides instructions on financial plans, apportionments, reappportionments, deferrals, proposed and enacted rescissions, systems for administrative control of funds, allotments, operating budgets, reports on budget execution, and reports on violations of the Antideficiency Act.
- h. OMB Circular A-123, Management Accountability and Control, requires agency management to assess, document, and report on internal controls over financial reporting.
- i. The DoC Accounting Principles and Standards Handbook prescribes accounting principles and standards to be followed within the Department in the design and operation of accounting systems, and it provides specific accounting principles and standards against which financial management and accounting systems can be evaluated and improved.
- j. The DoC Budget and Program Analysis Handbook contains policies and procedures governing the preparation and justification of the Department's budgets and the information and analysis necessary to meet the Secretary's responsibilities for managing the budget.
- k. Each fiscal year, the enacted Appropriations bill includes provisions that specifically address for that year the funding available for obligation and transfer to the NIST Working Capital Fund, reprogramming and other constraints, and additional reporting requirements.

Subchapter 8.04
Appropriated Funds
APPENDIX A

REQUIREMENTS UNDER THE ANTIDEFICIENCY ACT

The Antideficiency Act prescribes the legal requirements relating to apportionments, reappropriations, allotments, and expenditure controls, the fixing of responsibility and discipline for violation of such controls, and related reports. It states that "An officer or employee of the United States Government ... may not (a) make or authorize an expenditure or obligation exceeding an amount available in an appropriation ... or (b) involve ... Government in a contract or obligation for the payment of money before an appropriation is made" [31 U.S.C. 1341(a)(1)]. The Act also requires that certain appropriations be apportioned by months, calendar quarters, or other time periods or by activities, functions, projects, or objects in order to prevent over-obligation and to achieve effective and economical use of appropriations [31 U.S.C. 1512(b)(1)].

1. Violations

The following are reportable violations of the Antideficiency Act:

- a. To make or authorize an expenditure from or create or authorize an obligation under any appropriation or fund in excess of the amount available therein [31 U.S.C. 1341(a)];
- b. To authorize or create an obligation or make an expenditure in excess of an apportionment, reappropriation, or allotment [31 U.S.C. 1517(a)];
- c. To incur an obligation for payment of money for any purpose in advance of appropriations made for such purpose [31 U.S.C. 1341(a)]; and
- d. To accept voluntary services for the government or to employ personal services exceeding that authorized by law, except for emergencies involving the safety of human life or the protection of property [31 U.S.C. 1342].

2. Reports to the NIST Director

The Chief of the Finance Division is responsible for reporting in writing to the Director any over-obligation of an appropriation, apportionment, reappropriation, or allotment as disclosed by the accounting reports. This is done after consultation with the NIST CFO, the Budget Officer, and the NIST Deputy Director to determine and review all pertinent facts.

3. Reports to the Secretary of Commerce

The Director promptly reports all violations of the Antideficiency Act to the Secretary of Commerce through the DoC CFO. The report must be in the format and detail required by OMB Circular A-11, except that the report only recommends the administrative discipline to be imposed or other action to be taken with respect to the violator.

4. Administrative Discipline

The Secretary, or the Secretary's designee, determines the appropriate administrative discipline for violation of the Act and advises the NIST Director, who is responsible for administering the discipline. Statutory penalties for violations of the Antideficiency Act

Subchapter 8.04

Appropriated Funds

are provided in 31 U.S.C. 1349(a), 1350, 1518, and 1519. When circumstances warrant, appropriate administrative discipline includes but is not limited to suspension from duty without pay or removal. Criminal penalties for knowing and willful violation include a fine of not more than \$5,000, imprisonment for not more than two years, or both.

5. Reports to the President and Congress

The Secretary reports information on Antideficiency Act violations to the President, through the Director of OMB, and to the presiding officer of each House of Congress in the format and detail required by OMB Circular A-11.

OFFICIAL ENTERTAINMENT

Sections

8.09.01 Purpose

8.09.02 Scope

8.09.03 Policy

8.09.04 Delegation of Authority

8.09.05 Responsibilities

8.09.06 References

Appendix A - Entertainment Expenditures and Reimbursements

8.09.01

PURPOSE

This subchapter identifies activities which may be financed from: (1) gifts and bequests; (2) proceeds from their sale; or (3) income therefrom. Procedures for obtaining approvals and reimbursements are provided in Appendix A.

8.09.02

SCOPE

The procedures outlined in this subchapter apply to NIST-Gaithersburg and NIST-Boulder.

8.09.03

POLICY

Unrestricted or undesignated gifts (interest, donated funds, etc.) and gifts specifically designated for entertainment may be spent for entertainment purposes only when the expenditure aids or facilitates the work of NIST. Comptroller General Decisions B-142538 (February 8, 1961) and 46 CG 379 require that the justification must describe how the entertainment furthers the mission of NIST and how the NIST mission could not be accomplished as satisfactorily or as effectively without the expenditure. Approvals for the use of donated funds to cover expenses for entertainment are based on an administrative determination of necessity rather than desirability. The NIST Director may limit the activities approved based on availability of funds.

a. Entertainment costs must be charged to the special NIST-wide gift cost center. Any employee making unauthorized charges or charging entertainment to other cost centers is held liable for such charges and is required to pay the entertainment costs from personal funds.

b. Entertainment may be approved only if given for counterpart foreign dignitaries or officials and distinguished U.S. citizens who are involved in activities of specific, and not merely general, interest to NIST.

c. Authorization for use of the gift fund is primarily limited for use by the Visiting Committee on Advanced Technology and equivalent-level functions when authorized by the NIST Director.

d. Gift funds may be used to pay for meals, refreshments, or entertainment for all attendees only for those affairs where the attendance is predominantly distinguished visitors and the expenditure is approved by the Financial Operations Division.

e. Examples of activities for which entertainment expenditures may not be authorized are as follows:

(1) Entertainment to cultivate cordial relations, to manifest goodwill, or to reciprocate in kind hospitality extended by others to NIST employees;

(2) Conferences for which registration fees are levied;

(3) Entertainment for NIST employees and others (including guest researchers, Research Associates, visiting scientists/fellows, and summer employees) at functions such as award ceremonies, retirements, separations, orientations, social events, and work sessions;

(4) Meetings or conferences with employees of sponsoring government or private organizations to discuss currently sponsored, proposed, or completed work;

(5) Activities that could be construed as lobbying;

(6) Activities which could be embarrassing to the Secretary of Commerce;

(7) Printing of holiday or other greeting cards and business cards; and

(8) Payment for any alcoholic beverages.

8.09.04

DELEGATION OF AUTHORITY

Authority to approve the expenditure of gift funds for official entertainment has been delegated as follows:

a. For an amount exceeding \$1,000 on any one occasion, prior approval of the DoC Chief Financial Officer and Assistant Secretary for Administration is required.

b. For an amount \$1,000 or less on any one occasion, approval of the NIST Director is required.

8.09.05

RESPONSIBILITIES

a. The official who initiates the entertainment makes the initial determination that the request for approval of entertainment expenditures conforms with the policy stated in Section 8.09.03.

b. The Director, Office of International and Academic Affairs, certifies that foreign visitors are appropriate NIST counterparts for entertainment of foreign visitors.

c. The Deputy Chief Financial Officer/Financial Operations Division:

(1) Reviews requests for official entertainment expenditures;

(2) Ascertains whether sufficient funds are available;

(3) Determines whether requests are allowable under NIST guidelines;

(4) Forwards requests that meet the requirements to the Office of the Director; and

(5) Returns requests that do not meet requirements to the originating OU.

d. Staff making expenditures for official entertainment are responsible for:

(1) Obtaining a copy of the approval;

(2) Ensuring compliance with the approved request; and

(3) Attaching copies of the receipts and the approval to the document which requests reimbursement or accounts for any advance of funds obtained for the occasion.

8.09.06

REFERENCES

a. DAO 203-9, Gifts and Bequests.

b. DAO 203-10, Official Entertainment and Representation Authorizations.

c. Subchapter 8.10, Gifts and Bequests.

APPENDIX A

ENTERTAINMENT EXPENDITURES AND REIMBURSEMENTS

1. Requesting Approval for Expenditures

- a. For requests involving expenditures exceeding \$1,000 - The requesting OU prepares Form CD-464, Request for Authorization by Primary Operating Unit for Official Entertainment, for the NIST Director's signature. The requester forwards Form CD-464 (four copies) to the Deputy Chief Financial Officer/Financial Operations Division through the OU office (and the Office of International and Academic Affairs if foreign visitors are involved) for concurrence. The Financial Operations Division reviews the request and forwards it to the NIST Director.
- b. For requests involving expenditures of \$1,000 or less - The requesting OU prepares Form NIST-1099, Request for Authorization of Official Entertainment, and forwards Form NIST-1099 to the Financial Operations Division through the appropriate OU office (and the Office of International and Academic Affairs if foreign visitors are involved) for concurrence. The Financial Operations Division reviews the request and forwards it to the NIST Director.

The Office of the Director notifies the OU office of the approval or disapproval of the request.

2. Content and Timing of Request

The request for approval of expenditures must:

- a. State the nature of the entertainment for which approval is requested, its planned location, dates, number of persons invited, their titles or positions held, organizations they represent, and the reasons why such entertainment is being proposed, i.e., how it will aid or facilitate the work of NIST (see Section 8.09.03);
- b. Provide details of the estimated cost of the proposed entertainment including other associated expenses; and
- c. Be forwarded to the NIST Director through the Deputy Chief Financial Officer/Financial Operations Division according to the following schedule:
 - (1) For requests involving expenditures exceeding \$1,000, not less than three weeks in advance of the event (These requests must reach the DoC Chief Financial Officer and Assistant Secretary for Administration at least two weeks in advance of the event and are returned to the NIST originator without action if they cannot be processed through NIST in an orderly manner to meet that deadline.); or

(2) For requests involving expenditures of \$1,000 or less, five days in advance of the event.

3. Reimbursement of Entertainment Costs

a. When the NIST cafeteria serves meals or refreshments, it accepts from the host an approved Form NIST-1099. The NIST cafeteria submits the bill for the cost of the food served to the Financial Operations Division.

b. If meals or refreshments are to be provided at a restaurant on credit, the host must ask the manager, in advance, whether the restaurant will accept Form CD-435, Procurement Request. The host must submit Form CD-435 to the Purchasing Office for procurement action and handcarries the approved Form CD-435 to the restaurant. The restaurant must then submit a detailed bill to the Financial Operations Division.

c. If the host pays out-of-pocket or with a personal credit card, the host is reimbursed by submitting the approved request, with receipts attached, to the Imprest Fund cashier through the Financial Operations Division. Receipts are required for each expenditure over \$25.

d. Vouchers supporting expenditures shall include: (1) a copy of the approved request as specified in 1. above; or (2) a copy of the approved Form CD-210, Record Of Gift Or Bequest, as prescribed in Subchapter 8.10, Appendix A, when the gift was designated for specific entertainment.

e. If the host wants a cash advance of up to \$500, the host submits an approved entertainment request to the Imprest Fund cashier through the Financial Operations Division. The expenditures are then reconciled by submitting receipts to the cashier within five working days.

<p>U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY</p> <p>ADMINISTRATIVE MANUAL</p>	<p>Chapter 8 Financial Management</p>
	<p>Subchapter 8.10 Gifts and Bequests</p>

GIFTS AND BEQUESTS

Sections

8.10.01 Purpose
 8.10.02 Scope
 8.10.03 Policy
 8.10.04 Delegation of Authority
 8.10.05 Responsibilities
 8.10.06 Procedures
 8.10.07 Acknowledgment of Gifts
 8.10.08 Control and Reporting Requirements
 8.10.09 References
 Appendix A - Required Approvals for Gifts and Bequests
 Appendix B - Acceptance of Assistance-in-Kind from Domestic and Foreign Sources

8.10.01 PURPOSE

This subchapter implements at NIST, Department Administrative Order (DAO) 203-9 concerning the acceptance, use, and reporting of gifts and bequests made to the Department.

8.10.02 SCOPE

a. The procedures outlined in this subchapter apply to NIST-Gaithersburg and NIST-Boulder.

b. This subchapter does not apply to:

(1) Payment and acceptance of contributions, awards, or other expenses for training under Section 19 of the Government Employees Training Act of 1958 as amended (see DAO 202-410, Employee Development);

(2) Donation of personal services by individuals on a gratuitous or cooperative basis for advisory or other purposes;

(3) Contributions of funds, property, and services made and accepted pursuant to the Mutual Education and Cultural Exchange Act of 1961 as amended; and

(4) Transfers of funds to NIST from other federal agencies and direct payment of NIST employee travel expenses by other federal agencies.

8.10.03

POLICY

a. A gift may be accepted if the gift meets the following conditions:

- (1) It is expected to aid or facilitate some part or aspect of the work of NIST or the Department;
- (2) It would not involve in substance, or have the appearance of involving, personal benefit to an employee for or in contemplation of services to the donor;
- (3) Its acceptance would not tend to result in public misunderstanding concerning the ability of a NIST employee to carry out official duties in a fair, independent, impartial, or objective manner; and
- (4) Its acceptance would not reasonably be expected to result in impeding or otherwise impairing government efficiency or economy.

b. The gift or bequest should be free from restrictions, limitations, or control by the donor. A gift may be made for a particular investigation, development, or line of research, provided that the work to be performed is of a type which falls within the authorized functions of NIST. In addition, a gift may be made for purposes of official entertainment.

c. Gifts of money or property, other than for official entertainment, including the proceeds and income thereof, designated as to purpose are assigned to the Operating Unit (OU) concerned and are used as nearly as possible in accordance with the terms of the respective gift.

d. Gifts undesignated as to purpose are assigned to the Office of the Director. These funds may be used for official entertainment or for any other activities approved by the Director which fall within the authorized functions of NIST. Requests for use of such gifts for entertainment are made in accordance with Subchapter 8.09.

e. Gifts designated specifically for official entertainment are assigned to the Office of the Director and administered in accordance with Subchapter 8.09.

f. Employees should not accept for personal use gifts of cash or property offered for the performance of official duties.

g. Policies and procedures for acceptance of assistance-in-kind are detailed in Appendix B.

8.10.04

DELEGATION OF AUTHORITY

Prior approval by the following officials must be obtained before a gift can be accepted:

a. Secretary of Commerce - Gifts valued in excess of \$25,000.

b. Assistant Secretary for Administration

- (1) Real property or interest therein, regardless of value;
- (2) Gifts for work of the Department of Commerce in general, rather specifically for NIST, or if the gift is made specifically for NIST and other Commerce bureaus, regardless of the amount;
- (3) Gifts for activities not part of regular NIST programs, or which specify particular requirements as to deposit, investment, or management of fund, or which may require more than incidental expenditures for administration and use, or which otherwise may involve unusual conditions; and
- (4) Gifts in excess of \$100 for official entertainment.

c. NIST Director - Gifts of \$100 or less designated specifically for entertainment. (This authority cannot be

redelegated.)

d. Deputy Chief Financial Officer/Chief, Finance Division - Gifts not subject to prior approval of the Office of the Secretary or the Director, but subject to technical review by the division chief.

e. An individual employee may not accept for NIST honoraria or royalties for approved official activities. Any employee offered a royalty for editing or writing a publication should contact the Office of the Deputy Chief Counsel to ensure that an appropriate agreement for such services is executed prior to performing the work.

8.10.05

RESPONSIBILITIES

a. For gifts and bequests, the OU prepares (except as indicated in paragraphs c. and d. below) Form CD-210, Record of Gift or Bequest, which is used to obtain required approvals. Assistance-in-kind is specifically authorized in travel orders or administratively approved in travel vouchers. In all cases, the traveler reports the details of the receipt of assistance-in-kind on Form CD-210, Record of Gift or Bequest, a copy of which must accompany the travel voucher. Assistance-in-kind must be approved in advance. Exceptions may be made in extenuating circumstances and are approved on a case-by-case basis.

b. OUs receiving a gift offer notify the following so that required approvals may be obtained:

(1) Deputy Chief Financial Officer/Finance Division for offers of money;

(2) Acquisition and Assistance Division (AAD) for offers of property or equipment;

c. For offers of real property, the Plant Division prepares and forwards Form CD-210 to the Finance Division.

d. AAD prepares Form CD-210 for gifts of equipment and other personal property and forwards Form CD-210 to the Finance Division.

The organizational units mentioned above are also responsible for determining the value at which the donations are to be recorded.

8.10.06

PROCEDURES

a. Advance approvals required under Section 8.10.04 are obtained by the Finance Division using Form CD-210 after notification from OUs as specified in paragraph 8.10.05b.

(1) For gifts requiring Secretarial approval, the Finance Division:

(a) Prepares original and two copies of Form CD-210 for money, original and three copies of Form CD-210 for real and personal property;

(b) Routes original Form CD-210 to the Office of the Secretary through the NIST Deputy Chief Financial Officer and the Office of the Director, and

(c) After Secretarial approval, enters the accounting data on all copies of Form CD-210. (If property is involved, the original Form CD-210 is sent to the Plant Division or AAD as appropriate, and a copy is retained in the Finance Division.)

(2) For gifts for entertainment requiring the NIST Director's approval, the Finance Division prepares an original and three copies of Form CD-210 and forwards to the NIST Deputy Chief Financial Officer and Director for approval.

(3) For gifts not requiring approval by the Secretary or the Director, excluding honoraria and royalties, the Finance Division prepares an original and two copies of Form CD-210 and obtains required signatures, including the NIST Deputy Chief Financial Officer.

See Appendix A for a summary of approvals required.

b. Employees must not accept cash gifts under any circumstances. If cash is offered, the donor should be requested to make out a check or equivalent instrument payable to the National Institute of Standards and Technology. If a check or other instrument is made payable to the individual, it should be immediately endorsed to NIST, in the presence of the donor if practical, and forwarded to the Finance Division with Form NIST-776A, Transmittal Sheet for Cash Collections. The Finance Division issues Form NIST-110, Receipt for Monies Received by NIST from NIST Employee, to employees who receive payment for travel on official business, etc.

The original Form NIST-110 is to be attached to the employee's federal income tax return; a copy should be retained for their records. The monies involved should not be reported as income. Since the organization which made the payment may report it as income to the employee, attaching the receipt to the income tax return prevents inquiry from the Internal Revenue Service.

c. Employees may not accept personal gifts of property for the performance of official duties. The donor should be asked to title such property to the National Institute of Standards and Technology. If this is not feasible, the employee should transfer the property to NIST as soon as possible.

8.10.07

ACKNOWLEDGMENT OF GIFTS

All gifts should be appropriately acknowledged in writing. Except for monies, the acknowledgment shall not make reference to the value of the property/equipment received.

a. Initial Gift of \$1,000 or More - The OU Director sends a letter to acknowledge the gift. For unusual gifts, the letter may be prepared for the NIST Director's signature.

b. Subsequent Gifts from Same Donor for Same Purpose or Gifts for Less than \$1,000 - The Chief, Finance Division prepares and signs the letter subject to technical review by the appropriate OUs.

c. Miscellaneous Honoraria and Royalties - Individuals concerned should acknowledge as appropriate.

8.10.08

CONTROL AND REPORTING REQUIREMENTS

The following controls, reports, and records are to be maintained:

a. For gifts of accountable equipment received from nonfederal sources, AAD identifies donated equipment in the inventory records by placing the letter "G" following the inventory number on the inventory card. This identification ensures that proceeds from the disposal of gift equipment are retained in the Working Capital Fund (WCF).

b. The Finance Division:

(1) Records property, materials, and equipment in separate general ledger accounts and tracks them in separate property subsidiary ledgers;

(2) Deposits cash gifts in the appropriate receipt accounts using the NIST station symbol:

8501.1 Gifts and Bequests, Commerce

8501.2 Income on Investments, Gifts and Bequests, Commerce

(3) Uses the station symbol and the expenditure account symbol 13x8501, Gifts and Bequests- Commerce, when preparing vouchers to reimburse the WCF for costs incurred in gift cost centers; and

(4) Prepares and submits to DoC on a quarterly basis Standard Form (SF)-133, Report on Budget Execution.

(5) Prepares and submits to DoC on a fiscal year-end basis, a report showing the number, sources, nature, purpose, and amount of gifts and bequests; the nature and purpose of expenditures; and the annual investment income for the Gift Fund.

8.10.09

REFERENCES

- a. DAO 203-9, Gifts and Bequests, which prescribes policies and procedures for accepting gifts and bequests to the Department of Commerce.
- b. DAO 203-10, Official Entertainment and Representation Authorizations, which prescribes general guidelines for expenditures of funds for official entertainment and representation.
- c. Subchapter 8.09, Official Entertainment.

APPENDIX A

REQUIRED APPROVALS FOR GIFTS AND BEQUESTS

<u>Nature of Gift</u>	<u>Prior Approval</u>	<u>Approval Procedures</u>
1. Valued in excess of \$25,000.	Secretary of Commerce	Finance Division prepares Form CD-210, Record of Gift or Bequest, in triplicate and sends original to the Chief Financial Officer and Assistant Secretary for Administration through the NIST Director for Administration and Chief Financial Officer and the Office of the Director.
2. Real property or interest therein regardless of the value.	Assistant Secretary for Administration	Plant Division (at Boulder, Technical Services Division) prepares Form CD-210 in four copies and submits to the Finance Division which sends original to the Chief Financial Officer and Assistant Secretary for Administration through the NIST Director for Administration and Chief Financial Officer and Office of the Director. After approval, the NIST Deputy Chief Financial Officer/ Finance Division sends original to the Plant Division for Real Property records.
3. For work of DoC in general, rather than specifically for NIST, or if the gift is made specifically for NIST and other Commerce bureaus, regardless of the amount.	Chief Financial Officer and Assistant Secretary for Administration	Same as 1. above.
4. For activities not part of regular NIST programs, or which specify particular requirements as to deposit, investment, or management of fund, or which may require more than incidental expenditures for administration and use, or which otherwise may involve unusual conditions.	Chief Financial Officer and Assistant Secretary for Administration	Same as 1. above.

<u>Nature of Gift</u>	<u>Prior Approval</u>	<u>Approval Procedures</u>
5. In excess of \$100 for official entertainment (see Subchapter 8.09).	Chief Financial Officer and Assistant Secretary for Administration	Same as 1. above, except four copies are required. Form CD-210 must show purpose, occasion, dates, and persons to be entertained if known at time gift is offered. Furnish approved copy to requesting organizational unit for attachment to reimbursement request.
6. \$100 or less for official entertainment (see Subchapter 8.09).	Director (cannot be redelegated)	Finance Division prepares Form CD-210 in four copies showing information as in 5. above. Original to the Office of the Director for approval via the Deputy Chief Financial Officer. One copy to requesting organizational unit for attachment to reimbursement request.
7. Valued at \$25,000 or less and not involving gifts of types listed above.	Finance Division subject to technical review by the Director for Administration and Chief Financial Officer and OU Director for gifts in excess of \$1,000 and review by division chief for gifts of \$1,000 or less.	Finance Division prepares Form CD-210. For equipment or materials, the Acquisition and Assistance Division prepares Form CD-210 in four copies and forwards all copies to the Deputy Chief Financial Officer/Finance Division. Original is returned for filing in the Acquisition and Assistance Division.

APPENDIX B

ACCEPTANCE OF ASSISTANCE-IN-KIND FROM DOMESTIC AND FOREIGN SOURCES

A summary list of “DOs and DON’Ts” for the acceptance of assistance-in-kind appears at the end of this appendix.

1. Policies

- a. The authority to accept gifts in the form of prepaid tickets, lodging, meals, conference fees, or other assistance-in-kind is limited to NIST as an organization and cannot be extended to an employee. NIST may only accept assistance-in-kind with respect to attendance of an employee at a meeting or similar function relating to the official duties of the employee.
- b. NIST may only accept assistance-in-kind for NIST employees or for experts or consultants appointed under 5 U.S.C. § 3109. NIST is prohibited from accepting assistance in kind for contractors, whose services are received under procurement laws, and for Guest Researchers, foreign or domestic.
- c. Payment of employee travel expenses by other federal agencies is not assistance-in-kind and should not be reported on Form CD-210, Record of Gift or Bequest.
- d. Under no circumstances may a NIST employee accept a gift in the form of cash. If items received as assistance-in-kind are not paid for directly by the sponsor, the transaction should be completed as a reimbursement to NIST.
- e. Assistance-in-kind may not be accepted from private, for profit sources, from any foreign institution with which NIST is negotiating an agreement, or from any entity which is a grantee, contractor, or cooperative agreement partner with NIST. To identify donors with which there may be a conflict of interest, access the “vetting” checklist at: <http://www-i.nist.gov/admin/mo/adman/aikvetting.html>. (OU Senior Management Advisors are responsible for informing the Senior Management Advisor/Office of the Director, NIST, of any changes needed in this checklist.)
- f. The Operating Unit (OU) Director retains the authority to approve the acceptance of assistance-in-kind for any employee of their OU and may not delegate this authority. Assistance-in-kind for OU Directors may only be accepted by the Deputy Director of NIST. The Senior Management Advisor/Office of the Director, NIST, reviews the acceptance of assistance-in-kind and advises the OU Director on same.
- g. In the case of foreign sources, the Director, Office of International and Academic Affairs (OIAA), reviews the particular country and institution for consistency with current government policy.
- h. Employees are encouraged to contact the Counsel for NIST and/or OIAA if special circumstances exist or additional guidance is needed regarding the appropriateness of accepting assistance-in-kind from a domestic or foreign source.

2. Procedures

NOTES: (1) Prior to implementing the following procedures, refer to paragraph 1.e. above, and if the source is not obviously prohibited, complete the required vetting process. (2) Whenever possible, Form CD-210 or Form CD-342 should contain the actual, itemized amount of the gift from the sponsor as opposed to estimates of the gift based on government per diem rates.

- a. Domestic Sources - If a NIST employee receives an invitation from a domestic source offering assistance-in-kind, the employee must submit a completed Form CD-210, Record of Gift or Bequest; a copy of the letter, e-mail, or other communication documenting the invitation; and a completed Form CD-29, Travel Order, through: (1) line management as prescribed by the OU; (2) the Senior Management Advisor/Office of the Director, NIST; and (3) the Finance Division. On Form CD-210, the OU Director signs in Block 5 and the Senior Management Advisor/Office of the Director, NIST, signs in the COMMENTS section of Block 5. The OU must submit this information to the

Senior Management Advisor/Office of the Director, NIST, at least one week prior to the departure date of the travel.

b. Foreign Sources - If a NIST employee receives an invitation from a foreign source offering assistance-in-kind, the employee must submit a completed Form CD-210, Record of Gift of Bequest, or Form CD-342, Record of Gift From a Foreign Government; a copy of the letter, e-mail, or other communication documenting the invitation; and a completed Form CD-29, Travel Order, through: (1) line management as prescribed by the OU; (2) the Senior Management Advisor/Office of the Director, NIST; (3) the Director/OIAA; and (4) the Finance Division. On Form CD-210, the OU Director signs in Block 5 and the Senior Management Advisor/Office of the Director, NIST, and the Director/OIAA sign in the COMMENTS section of Block 5. On Form CD-342, the OU Director signs in Block 6 and the Senior Management Advisor/Office of the Director, NIST, and the Director/OIAA sign in the COMMENTS section of Block 6. The OU must submit the required information to the Senior Management Advisor/Office of the Director, NIST, at least three weeks prior to the departure date of the travel.

c. On occasion, a NIST staff member may not have been aware in advance that assistance-in-kind was to be offered. In such cases, the gift may be accepted if the conditions in paragraph 1. above are met. Within fifteen working days after the traveler's return, the appropriate paperwork must be completed and submitted in accordance with paragraph a. or b., as appropriate. The package must include a memorandum explaining the circumstances under which the gift was offered and a justification for not having had it approved in advance.

DOs AND DON'Ts

DOs:

DO submit AIKs on the proper form.

DO submit AIK forms as early as possible to allow for processing time.

DO include actual, itemized figures for the travel gift, rather than estimates based on government per diem rates.

DO feel free to accept gifts of \$20 or less (\$50 annually) from any source at any time. Such nominal gifts are not considered AIK and do not require an AIK form.

DO accept waiver of conference fees on days when speaking at an event, as well as any food and entertainment provided to attendees as part of the event. These are not considered AIK and do not require an AIK form.

DO determine whether the foreign institution from which a gift is received is a government entity. Foreign universities are often considered to be governmental for these purposes.

DO be aware of whether the foreign institution or country where traveling has politically sensitive issues with NIST.

DO contact the Counsel for NIST for additional guidance as needed.

DON'Ts

DO NOT accept AIK from any current or imminent grantee, contractor, or cooperative agreement partner of NIST.

DO NOT accept AIK from any for-profit entities.

DO NOT accept cash gifts under any circumstances. Also, checks should be made payable to NIST and not to individual travelers.

EQUIPMENT FINANCING

Sections

8.11.01 Purpose

8.11.02 Scope

8.11.03 Legal Authority

8.11.04 Policy

8.11.05 Delegations of Authority

8.11.06 Definitions

8.11.07 Responsibilities

8.11.08 Procedures

8.11.09 Content Owner

8.11.10 Effective Dates

Appendix A - Equipment Installation and Manufacture

Appendix B - Instructions for Purchase vs. Lease Cost Analysis

Appendix C – WCF Invested Equipment Financing/Allocation Process

8.11.01

PURPOSE

This subchapter states policies for: financing the acquisition of equipment; determining whether to purchase or lease the equipment; recording costs for manufacture of equipment; acquiring and financing computer software; and making loan repayments on Working Capital Fund (WCF) Invested Equipment (IE). See Subchapter 7.01 for information on equipment accountability and control.

8.11.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

8.11.03

LEGAL AUTHORITY

NIST can retain net earnings in the WCF to restore prior losses and to ensure the availability of capital necessary to replace equipment and inventories. In addition, NIST may retain all building use and depreciation surcharge fees collected pursuant to OMB Circular A-25. Any additional earned income

resulting from the operation of the WCF must be paid to the general fund of the Treasury. For more information, see:

Pub. L. 81-583

15 U.S.C. 278b

15 U.S.C. 275c

15 U.S.C. 278d(b)

8.11.04

POLICY

It is NIST policy that equipment needs are normally filled as an investment of the WCF. Exceptions to this policy are contained in Section 8.11.06. Funds for investment are obtained from the appropriation process, from monthly repayments on WCF IE loan balances, and from an equipment replacement surcharge.

8.11.05

DELEGATIONS OF AUTHORITY

Subject to any special approvals outlined in Subchapter 2.03, Procurement, the following approval procedures apply:

- (1) Equipment costing less than \$5,000 is approved within the OU.
- (2) Equipment costing from \$5,000 to \$100,000 may be approved by the OU Director or this authority may be redelegated to division chiefs, Senior Management Advisors (SMA), and program managers by the OU Director.
- (3) Equipment costing \$100,000 or more requires the approval of the OU Director.
- (4) Equipment costing \$500,000 or above and/or any amendment that would increase the original cost of the equipment to equal \$500,000 or above requires the approval of the NIST Deputy Director.

8.11.06

DEFINITIONS

a. Acquisition Cost - The full cost incurred to bring a piece of equipment to a form and location suitable for its intended use, including all costs related to acquisition, delivery, and major installation costs (See Appendix A).

b. Computer Software - Software includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program. "Internal use software" means software that is purchased from commercial vendors "off-the-shelf", internally developed, or contractor-developed solely to meet the entity's internal or operation needs. Normally software is an integral part of an overall system(s) having interrelationships between software, hardware, personnel, procedures, controls, and data. Software is classified in the accounting system using object class 31.25 (capitalized) and object class 31.55 (expensed).

c. Equipment - Non-expendable property, such as computers, office, shop, and scientific and technical equipment, which is complete in itself, and is of a durable nature. Equipment can be either capitalized or expensed on the NIST financial statements. All equipment with an acquisition cost of \$5,000 or more, or that is part of a system totaling at least \$5,000, or equipment classified as personal appeal, is subject to inventory control by the Personal Property Office.

d. Capitalized Equipment has an initial acquisition cost of \$25,000 or more and an estimated useful life of two years or more.

(1) Depreciation - Depreciation expense is recorded in the NIST Accounting System and reflected on the NIST financial statements for all capitalized equipment, regardless of source of funding. The purpose of depreciation is to spread the acquisition cost over the useful life of the equipment; NIST calculates depreciation using the straight-line method.

(2) Useful Life - The estimated number of years the equipment normally functions adequately before it wears out, becomes technologically obsolete, or the project for which the equipment was acquired is completed if the equipment is not likely to be used in other projects. Useful life is used to determine the depreciation expense on capitalized equipment. See Subchapter 7.01 Appendix B, Useful Life - Depreciation, for standard useful lives.

e. Expensed Equipment has an initial acquisition cost less than \$25,000 or an estimated useful life of less than two years.

f. WCF IE – The funding source primarily used by NIST to purchase equipment, especially when it benefits both internal and external customers. OUs should generally use IE funding if the cost of the equipment is over \$5,000 and the equipment will have a useful life of more than one year. Obligations and accruals for direct purchases are recorded in project types IEDISC or IESPC (in the series 800-805 and 806-809, respectively). Obligations and accruals for manufactured equipment are recorded in project types MANDIS or MANSPC (series 810-844 and 845-849, respectively).

(1) WCF IE Allocations - Permission to purchase or manufacture equipment with Working Capital Funds is granted to OUs by the NIST Director, in the form of a WCF IE allocation (see Appendix C).

(2) Loan Repayments and Surcharges - The WCF is repaid for each piece of equipment purchased using WCF IE through monthly loan repayments (object class 61.27, 61.28, and 61.29) and surcharges (object class 61.30) which are generally applied to overhead projects.

g. Unfinanced Equipment - Equipment not acquired as an investment of the WCF, generally costs less than \$5,000, or otherwise meets the criteria for non-WCF IE provided in Section 8.11.08a. The acquisition cost is charged directly to the project creating the need for the equipment.

8.11.07

RESPONSIBILITIES

a. The Budget Division and Finance Division are responsible for establishing policies for financing equipment and monitoring spending against authorizations.

b. The Budget Division:

(1) Advises the CFO as to the amount and allocation of Working Capital Funds to be made available for investment in equipment, which are based on the anticipated loan repayments in a given fiscal year, unobligated balances, and new initiatives.

(2) Ensures that equipment needs (WCF and non-WCF) associated with new budget initiatives are included in budget submissions;

- (3) Reviews estimates to confirm that each OU has adequate long-term funding to repay the WCF for new equipment investments;
- (4) Authorizes WCF IE projects (IEDISC, IESPC, MANDIS, MANSPC);
- (5) Makes recommendations on special requests for WCF IE allocations; and
- (6) Monitors spending against authorization for each WCF IE allocation.

c. The Finance Division:

- (1) Calculates the maximum amount of Working Capital Funds that can be invested in equipment each year;
- (2) Administers the loan repayment process; and
- (3) Ensures that NIST procedures and policies are in compliance with DoC policies and that NIST financial statements are prepared according to generally accepted accounting principle

8.11.08

PROCEDURES

a. Financing

(1) WCF IE - Equipment costing at least \$5,000 should be acquired as an investment of the WCF unless it meets one of the criteria below for non-WCF IE. This mechanism was established to permit appropriate costing of the equipment over its lifetime and to ensure that adequate replacement funding will be available. Guidelines for financing the acquisition of equipment using Working Capital Funds are provided in Appendix C.

(A) Two or more OUs/divisions may pool their WCF IE allocations to purchase a single piece of equipment for their mutual use. The purchase order must contain all OU/division acquisition projects that are sharing the cost of the asset; this requirement enables the Finance Division to correctly calculate each OU's/division's IE loan balance.

(B) Equipment may be jointly funded by WCF IE and another source of funding. If federal government/ non-federal government/ CRADA sources are used, the consent of the sponsor is required. Loan repayments are recovered only on that portion of the cost funded from the WCF IE. The portion of the total cost funded by a non-WCF source is charged directly to that specific project.

(2) Unfinanced Equipment - Equipment costing less than \$5,000, and other instances, as stated below, may be charged directly to the project(s) creating the need for the equipment.

(A) Appropriated or Overhead funds should be used when one of the following conditions is met:

- (i) The equipment costs less than \$5,000

(ii) Equipment will be consumed, destroyed, contaminated, modified, or lose its original identity so as to render it useless at the completion of the task(s) for which it was originally purchased and would be declared surplus at that point.

(iii) The utility of the equipment is so specific as to be limited to only the technical project for which it is initially purchased.

(iv) The OU/division/group only has appropriated funding.

(v) Books, regardless of price, which are purchased for the permanent collection of the NIST Information Services Division are coded as equipment. This classification as equipment is dictated by guidelines established by the Office of Management and Budget. Books purchased for other than the NIST Information Services Division are coded as Supplies (object class 26.0).

(B) Federal Government/Non-Federal Government/CRADA Projects

Equipment may be purchased with federal government/non-federal government/CRADA funds in the project(s) creating the need for the equipment rather than as an investment of the WCF, unless the federal government/ non-federal government/CRADA order contains a statement which specifically precludes equipment purchases. Consent of the sponsor is required and it is preferable that special equipment requirements be stated in the federal government/non-federal government/CRADA order.

(C) Expense and Income Projects

(i) Equipment may be charged to Miscellaneous Expense and Income projects (project types MSCFED, MSCSTL, or FDLBCN, series 585-594) without regard to price or useful life provided that the sponsor(s) (government or nongovernment) has given implicit or explicit permission to purchase or manufacture such equipment.

(ii) Equipment may not be charged to other Expense and Income projects (project types INTDIV, CALPGV, TSTSTL, TSTFED, SRMOPR, SRMSAL, SRMSDS, PROPME, CALOPR, or CALSDS, series 595-699) that are reimbursed through fees established for conferences, training classes, calibrations, SRMs, or tests. Any exceptions to this policy must be approved by the Budget Division and the Finance Division.

b. Purchase vs. lease determination - Requests for the acquisition of equipment should be carefully evaluated to determine whether it is more economical to purchase or lease.

(1) The Federal Property Management Regulations and the General Accounting Office recommend leasing equipment only when there is a cost savings. The determination to lease rather than to purchase must be fully justified.

(2) To evaluate whether it is more economical to lease or purchase items of significant value, the requesting organizational unit assists the contracting officer in performing a cost comparison for lease vs. purchase. All requisitions for the lease of an asset valued at over \$100,000 must be accompanied by a cost analysis and justification which has been reviewed and approved by the

Chief Financial Officer (CFO). The worksheet and instructions on the comparative cost analysis spreadsheet that should be used in this analysis is located at http://www-i.nist.gov/admin/dcfo/budget/lease_purchase.html. The following factors should be considered when undertaking a comparative cost analysis:

- (A) Length of time that the equipment is to be used, including extent of usage and potential additional use by another federal agency if the equipment becomes excess to the acquiring agency;
- (B) Financial and other advantages of all types and makes of equipment available;
- (C) Leasing costs and purchase options;
- (D) Purchase costs of new equipment, including similar equipment or equipment of a different type and make;
- (E) Costs of installation and maintenance;
- (F) Imminent technological improvements; and
- (G) Other pertinent factors.

(3) OMB Circular A-94 applies when the lease-purchase analysis concerns a capital asset or a group of related assets whose total fair market value exceeds \$1 million.

c. Means of Acquiring Equipment

- (1) Purchase - If it is more economical to purchase rather than to lease.
- (2) Manufacture of Equipment - The cost to manufacture WCF IE is accumulated in Project Types MANDIS and MANSPC. Research and development costs are not included (see Appendix A, paragraph 2.d.).
- (3) Equipment Purchased After Initial Rental - The cost placed on the property records is the purchase order price.
- (4) Equipment Purchased with a Trade-In - Prior approval from the Administrative Services Division must be obtained before a trade-in can occur. The cost placed in the property records is the full purchase price including the value of the trade-in.

d. Computer software acquisition and financing

- (1) Purchased computer software is considered to be equipment by OMB guidelines and is assigned object class 31.25 for capitalized ADP Software, 31.23 for Internal Use Software in Development or 31.55 for non-capitalized ADP Software.
- (2) Software may be purchased with an OU's WCF IE allocation only in the following circumstances:

(A) The software is general purpose in nature and applicability and its expected life is two years or more and its cost is \$5,000 or more. The property records will be adjusted to include the software cost with the cost of the computer on which it is to be used; and/or

(B) The software is acquired at the same time as computer hardware that is also purchased as WCF IE.

(3) Software not meeting the above requirements is charged as a current operating expense to the benefiting project(s).

(4) Costs for software developed in-house are either charged as a current operating expense or capitalized under the requirements of Statement of Federal Financial Accounting Standards (SFFAS 10) – “Accounting for Internal Use Software”. Working Capital funds are not used to develop software in-house.

(5) Capitalization - The Finance Division capitalizes software according to the requirements of SFFAS 10.

e. Loan repayments

(1) Special IE Funds – The Budget Division allocates IE funds stemming from new budget initiatives and for projects selected in the annual Innovations in Measurement Science (IMS) competition. Project types used for Special IE projects are IESPC and MANSPC. Repayments are due from OUs to the WCF in equal installments over seven years, beginning the year after obligation.

(2) Discretionary IE Funds - Each OU is allocated a line of credit in Discretionary IE funding. An OU's Discretionary IE loan balance is subtracted from the line of credit to determine the OU's Discretionary IE availability (i.e. funds available for obligation). As funds are obligated, the OU's loan balance increases and the IE availability decreases. As funds are repaid, the loan balance decreases and the IE availability increases. Although the funds management and repayment schedule for Discretionary IE remains in the control of the OU, the loan balance can never exceed the line of credit. Project types used for Discretionary IE projects are IEDISC and MANDIS.

(3) During October of each year, the Finance Division will provide a loan repayment planning worksheet to each OU. Information provided on the worksheet will include Special IE (Initiative and IMS) loan balances and mandatory repayment schedules, and Discretionary IE lines of credit and loan balances, with loan repayment amounts left blank. Each OU will return the worksheet to the Finance Division after filling in the loan repayment project codes (ACCS) and the amounts to be repaid on discretionary loan balances. The Finance Division will use the repayment planning worksheets to post the appropriate general ledger entries.

(4) IE Loan Balance Reports are available on the CBS Portal and can be generated by the OUs as needed. These reports are available for IE Discretionary and IE Special (Initiative and IMS) in both Summary and Detail formats. The reports provide Line of Credit and Loan balance information as well as year-to-date loan payments and remaining payments for the fiscal year.

(5) NIST has statutory authority to retain and use earned net income to offset the effects of inflation on equipment and inventories. Since the cost of equipment continues to increase, a surcharge using object class 61.30 is added to the regular loan repayment charge. This surcharge

collects the estimated additional cost associated with replacing equipment in the future. See “User Information” on the CFS Home page for the current IS rate.

8.11.09

CONTENT OWNER

161 – Budget Division and 162 – Finance Division

8.11.10

EFFECTIVE DATE: 8/11/2009

APPENDIX A

EQUIPMENT INSTALLATION AND MANUFACTURE

1. Installation Costs

- a. Equipment is recorded at full cost, which includes installation costs that are material. Installation includes those functions necessary to put a piece of equipment in operable condition, such as utility connections, ductwork, and pedestals. Not included are costs for the modification of the basic equipment, connection of separately capitalized auxiliaries, attachment of experimental setups, or other special arrangements necessary to adapt the equipment to its initial program use.
- b. Installation costs are added to the acquisition cost of equipment the first time a piece of equipment is installed and put into operation. Moving and installation costs after the original installation are not added to the acquisition cost.
- c. Requisitions for equipment that may require construction or installation of utility services are routed through the Plant Division to ensure that the equipment can be installed properly.
- d. When the NIST Plant Division installs equipment on a fixed-price basis, the organizational unit acquiring the equipment must designate on Form NIST-461, Interdivision Work Order, the project (excluding manufacture of IE series) and purchase order number on which the equipment was acquired. The Plant Division sends the Administrative Services Division a copy of the work order indicating the amount to be added to the equipment purchase price to establish capital value.
- e. If the installation is not handled on a fixed-price basis, then a manufacture of WCF IE project should be established to accumulate the costs of the basic equipment and the installation.

2. Manufacture of WCF IE

- a. Individual projects are established in the manufacture of WCF IE series (810-849, project types MANDIS and MANSPC) to accumulate the labor and other object costs of each piece of equipment to be constructed. If more than one piece of identical equipment is to be made, a single project may be established for accumulating costs. These projects are funded out of the requesting OU's WCF IE allocation. Manufacture of equipment projects should only be established when there is going to be a tagged piece of property at completion.
- b. To establish new manufacture of WCF IE projects, the originating organizational unit must forward a completed Form NIST-635, Request for Authorization of Manufacture of WCF IE, to the Budget Division. Once approved, the Budget Division then forwards a signed copy of Form NIST-635 to the Finance Division. Form NIST-635 should also be used for subsequent changes to the resources and/or end date for an established manufacture of WCF IE project. The form must be received and approved before any obligations/costs may be incurred.

Form NIST-635 is used to justify and identify costs of equipment to be manufactured. The information provided on Form NIST-635 is used by the Budget Division in programmatic review and approval of the initial allocation of manufacture of equipment projects and reallocation in subsequent years. The information also assists the Finance Division in timing its requests for Form

NIST-409, Notice of Completed Manufactured Equipment, which is prepared by the originating organizational unit.

c. Research and development costs may not be charged to manufacture of equipment projects. The cost of the design, preparation of specifications and drawings, and costs of a similar nature incurred directly in the manufacture may be charged to a manufacture of equipment project if they can be segregated from research and development costs.

d. Upon completion of the equipment:

(1) The organizational unit responsible for the manufactured equipment submits a Form NIST-409, Notice of Completed Manufactured Equipment, to the Finance Division.

(2) The Finance Division validates the cost in the accounting system to the amount on the Form NIST-409 and sends a copy to the Administrative Services Division. The Administrative Services Division assigns a NIST tag number(s) to the equipment and notifies the Finance Division in order for them to complete the capitalization process.

e. If the equipment is not completed for any reason, then the project is terminated and all costs incurred must be transferred to a non-WCF Invested Equipment project(s).

f. Spending in each WCF Invested Equipment (IE) project must be kept within its authorized level. If the total cost of manufacturing the equipment exceeds the authorized amount, the overrun must be covered by reassigning additional WCF IE authorization from other WCF IE projects within the same discretionary or special series in the OU.

g. Any funding balance remaining in a Discretionary IE manufacture of equipment project (MANDIS) after completion of the equipment is available in the OU Discretionary IE line of credit. Any funding balance remaining in a Special IE manufacture project (MANSPC) must be approved by the Budget Office before it can be carried forward into the next fiscal year.

APPENDIX B

INSTRUCTIONS FOR PURCHASE VS. LEASE COST ANALYSIS

General Instructions:

- An electronic spreadsheet is available for downloading at the Chief Financial Officer's website which is located at http://www-i.nist.gov/admin/dcfo/budget/lease_purchase.html or a file can be obtained from the Reconciliations Group, Finance Division.
- The analysis needs to be performed when considering whether to lease rather than purchase an asset valued at more than \$100,000.
- The initial determination of purchase vs. lease should be made based on market research information obtained by the requisitioner. Data source and assumptions should be noted in the comments section.
- The user should input the requested information into the shaded areas of the spreadsheet.
- Approval of the analysis will be determined by the Chief Financial Officer based on information submitted by the requisitioner. After Chief Financial Officer approval, the Cost Analysis spreadsheet will be sent back to the requisitioner to be combined with the requisition and forwarded to the Acquisition Management Division for action.
- Before finalizing a lease, the Acquisition Management Division compares information from the cost analysis with the actual proposal received from the vendor. If the Net Present Value of both the lease payments and the purchase price are within ten percent of the requisitioner's original quotes, then the procurement official may proceed with the procurement. If not, then the Chief Financial Officer's approval of the lease based on the final quote calculations is required.
- Line by line instructions are provided with the worksheet.

APPENDIX C

WCF INVESTED EQUIPMENT FINANCING/ALLOCATION PROCESS

1. Funds for WCF IE

Working Capital Funds for investment in equipment are obtained through the appropriation process and by the recovery of previous investments through monthly loan repayments and surcharges. The appropriation may include two types of increases for equipment funding: (1) adjustments to base to finance increased costs for replacing equipment; and (2) equipment requirements identified with budget initiatives.

To keep pace with the rising costs of equipment, a surcharge is added to the monthly loan repayments. The surcharge is determined by general price level adjustment data and reviewed annually by the Budget Division (see CBS Portal Homepage for the current surcharge rate).

2. WCF IE Allocations

a. Allocation Categories

(1) Initiative: Equipment for approved budget initiatives, funded by appropriation transfers to the WCF as specified in the initiative pricing and authorized by Congress.

(2) IMS: Resources allocated from the WCF IE by the NIST Director for equipment needs relating to Innovations in Measurement Science (IMS) projects.

(3) Discretionary: Equipment for the on-going operation of the OU. Distribution of funds within the OU is at the discretion of the OU Director.

b. Request and Allocation: The total funding allocation for WCF IE is based on several factors, including estimated loan repayment and surcharge collections, WCF transfers for budget initiatives, and prior WCF commitments.

(1) Category - Initiative

Manner of Request - Must be included in initiative pricing.

Allocation - Following appropriation and transfer to the WCF.

(2) Category - Special IMS

Manner of Request - Annual Innovations in Measurement Science proposals.

Allocation - Following NIST Director's selection of the awards.

(3) Category -Discretionary

Manner of Request - OUs determine and provide their annual loan repayment estimates to the Finance Division

Allocation - At the start of each fiscal year.

c. Monitoring of Spending:

(1) OUs are responsible for ensuring that spending is kept within authorized levels and for returning excess funds, if applicable, in a timely manner.

(2) The Budget Division and the Finance Division monitor spending on a monthly basis.

(3) Rate of spending is reviewed by the Budget Division with each OU on a quarterly basis.

d. Actions to Ensure Utilization: In early April, following the close of the second quarter, the Acquisition Management Division provides each OU with a status report on procurement items that might encounter award difficulties.

e. Unobligated Balances:

(1) Special Initiative and Innovations in Measurement Science Invested Equipment end-of-year unobligated balances greater than \$1,000 carry over for the source OU if there is a continuing need.

(2) Discretionary Invested Equipment end-of-year unobligated balances become part of the available balance for the source OU the following fiscal year.

f. Adjustments to Discretionary Allocation:

(1) Other Adjustments to Discretionary Allocation: In response to unique program requirements or major budgetary shifts, it may become necessary for the Director to make adjustments on a permanent basis to the OU discretionary levels. In these cases, the discretionary Line-of-Credit for each OU is adjusted to reflect the change and discretionary allocations are based on estimated loan repayments on the adjusted figures.

OFFICIAL TRAVEL

Sections

- 8.12.01 Purpose
- 8.12.02 Scope
- 8.12.03 Legal Authority
- 8.12.04 Policy
- 8.12.05 Delegations of Authority
- 8.12.06 Responsibilities
- 8.12.07 Procedures
- 8.12.08 Content Owner
- 8.12.09 Effective Date
- Appendix A – Travel References
- Appendix B – Year End Travel Processing
- Appendix C – Common Carrier Transportation Purchases
- Appendix D – Relocation Forms

8.12.01 PURPOSE

The purpose of this subchapter is to outline National Institute of Standards & Technology (NIST) internal policies and procedures for official travel. This subchapter incorporates by reference the Federal Travel Regulation (FTR) issued by General Services Administration (GSA), the Commerce Travel Handbook (CTH) issued by the Department of Commerce, Office of Administrative Services (OAS), Travel Management Division (TMD), and Title 5, Chapter 57 of the United States Code. (See Appendix A.)

8.12.02 SCOPE

The policies and procedures contained in the Federal Travel Regulation, the Commerce Travel Handbook, and this NIST Administrative Manual subchapter are applicable to all NIST employees and invitational travelers performing official Government travel on behalf of the Department of Commerce, NIST.

8.12.03 LEGAL AUTHORITY

United States Code, Title 5, Chapter 57
41 CFR Subtitle F--Federal Travel Regulation System (Parts 300-304)

I. Temporary Duty (TDY) Travel Allowances

A. Applicability

The order of applicability for travel regulations is as follows: 1) GSA-FTR, 2) DOC-CTH, and 3) NIST-Admin Manual Travel subchapter. NIST policies may only further define travel entitlements. Under no circumstances may the NIST policies supersede or override the law pertaining to Federal travel or regulations established by GSA and/or DOC.

All official travel must be held to the minimum consistent with the requirements of official business. Only those travel and transportation expenses essential to performing the agency mission may be authorized as official travel.

B. General Rules

1. Travel Authorizations

- a. Travel authorizations for employees and invitational travelers performing official Temporary Duty Travel (TDY) or Long Term Travel will be prepared in Travel Manager.
- b. Travel authorizations must be issued in advance of travel except in extreme emergency cases. See CTH C300(c) and C301-2.1.
- c. Travel expenses incurred due to a traveler's personal preference or convenience will be the responsibility of the traveler.

2. Amendments to Travel Authorizations

Amendments should be performed if one or more of the following circumstances occurs:

- a. Travel costs will be materially affected (+ \$250)
- b. Changes in the itinerary (location)
- c. The travel dates change by 30 days or more
- d. Required justifications were not included on the original authorization
- e. The document is rejected by the accounting system and the NIST Travel Office notifies you that changes are necessary

Note: Amendments should not be issued after the travel has been started or completed. If expenses are incurred that were not included on the original authorization, they must be post-approved on the travel voucher.

3. Recurring Expenses

Recurring expenses may be used on the travel authorization to estimate the travel expenses to be obligated but all expenses must be itemized on the travel voucher.

Recurring expenses consist of the following:

- a. Taxi to and from the airport
- b. POV mileage to and from the airport
- c. Airport parking
- d. Tolls
- e. Copies

4. Cancellation of Travel

If travel must be canceled, the following steps should be taken:

- a. Notify the Travel Management Service (TMS) provider (Adtrav) so that common carrier tickets, rental car, and hotel reservations may be canceled. Return any unused paper tickets to the TMS provider.
- b. Notify the Travel Office by sending an e-mail to travelof@nist.gov. The e-mail should state the name of the traveler, document number, and reason for cancellation. The travel authorization will be canceled in Travel Manager (if applicable) and funds will be deobligated as necessary.

Note: If the traveler has incurred any expenses (ex: POV mileage driving to and from the airport), do not cancel the order through the Travel Office. The obligation must remain in place until the voucher is processed.

5. Contractor Travel

Under no circumstances may contractors be issued travel authorizations, use the Government contract city-pair fares, or charge common carrier transportation to the Centrally Billed ticket account for NIST. Required travel costs for contractors must be included in the overall contract price and paid under the contract.

6. Group Travel

Group travel is defined as "groups of employees from the same bureau/operating unit, including non-Government persons (invitational travelers) whose travel expenses are being paid for by the Department [of Commerce], traveling to the same location or event." Group travel consists of the following: for travel **within** the continental United States, the approval will be for groups of **fifteen or more**. For travel **outside** the continental United States, the approval will be for groups of **eight or more**.

- a. The authority to approve group travel has been delegated to the Operating Unit (OU) Directors.

- b. NIST must maintain sufficient documentation, signed by an appropriate official, to demonstrate compliance with the minimum standards in selecting locations or attendees. NIST Operating Units are responsible for maintaining appropriate records indicating review and approval by the OU Director. These records are subject to review by DOC upon request. After the OU Director approves the group travel memorandum, it must be forwarded to the Travel Office, Mail Stop 1622, 101/A935.
- c. Minimum Standards for Approval of Group Travel

The following standards shall be followed when approving group travel:

- a. Ensure that only travel that is essential to the purposes of the Department and for accomplishment of NIST's mission is approved.
- ii. Ensure that NIST attendance is limited to the minimum necessary to accomplish the mission.
- iii. Consider all expenses in selecting attendees and conferences or meeting locations. Such expenses include travel to and from the site, ground transportation, lodging, meals and incidental costs, registration fees, meeting room rentals, and other related costs including employees' time away from their official duty station.
- iv. Explore alternatives to holding conferences or meetings away from the NIST sites, such as conference calls, teleconference or having available field personnel accomplish the proposed mission.

7. Personal Leave Taken In Conjunction with Official Travel

- a. Government contract city-pair fares may not be used for personal travel.
- b. Authorization for a traveler to take personal leave in conjunction with official travel is at the discretion of the approving official.
- c. When a traveler requests annual leave during a period of official travel, the comments section of the travel authorization must include the places and dates of the planned leave.

8. Begin/Ending Point of Travel

- a. According to FTR 301-10.7, NIST employees and invitational travelers must travel to their destination by the usually traveled route unless NIST authorizes or approves a different route as officially necessary.
- b. On a case-by-case basis, an employee may be authorized to begin or end travel at a point that is not the employee's official duty station or temporary duty station using government or contract fares as long as it is advantageous to the government.
- c. This authority must be closely monitored to avoid the appearance that the Government is

subsidizing an employee's personal travel.

- d. If the traveler chooses to travel by an indirect route, the reimbursement will be limited to the cost of travel by a direct route or on an uninterrupted basis. The traveler will be responsible for any additional costs.

9. Defensive Travel Briefing for Foreign Travel

- a. Travelers that perform official foreign travel are required to take the Defensive Travel Briefing training annually.
- b. Information regarding travel security may be obtained on the DOC/Office of Security website at <http://home.commerce.gov/ocy/default.htm> .
- c. For guidance regarding the official usage of government-owned computers and personal digital assistants (PDA) while on official travel contact the NIST ITAC Help Desk at x5375.

C. Transportation Expenses

1. Common Carrier Transportation

- a. Electronic tickets will be issued for common carrier transportation. The only exception to issuance of electronic tickets is if a vendor or locale does not offer electronic ticketing services. In these limited instances where there is no other alternative; the Government will cover the cost of issuing the paper ticket.
- b. Travelers requesting issuance of paper tickets for personal preference or convenience when e-tickets are available will be responsible for any additional cost incurred.

2. Airline Accommodations

- a. Coach-class – Is the preferred method of transportation.
- b. Business-class – When officially necessary and justified, travelers may be authorized to upgrade to business class in accordance with 301-10.124 of the FTR. Additionally, a traveler may upgrade to business class at their own personal expense (including through the redemption of frequent flyer miles).
- c. First-class – Under normal circumstances, DOC policy does not allow authorization of first class. (See CTH 301-10.123(a) & (b).) In extreme emergency circumstances, (i.e., disability, no commercial service is reasonably available within 24 hours, or exceptional security), exceptions may be made with proper justification.

3. Medical Certifications

- a. All travel exceptions requested and authorized based on medical necessity must be substantiated in writing by a competent medical authority.

- b. Medical certifications must be recertified every two years.

4. Government Automobiles

Contact the NIST Transportation Services Group at x5922 or x5923 for vehicle availability and policies regarding the usage of Government vehicles on official travel.

5. Privately Owned Vehicle (POV)

- a. Approving Officials cannot require travelers to use their POV to perform official travel.
- b. POV maintenance and operating expenses, such as tires, oil changes, replacement parts, speeding tickets, etc., are not reimbursable as travel expenses.

6. Cost Comparison

- a. When use of common carrier is authorized but a traveler chooses to use their own POV for reasons of personal preference or convenience, a constructed cost comparison must be prepared by the secretary or traveler and approved by the authorizing official.
- b. Regardless of the mode of transportation the traveler chooses, the reimbursement to the traveler will be limited to the amount that results in the greatest cost savings to the Government.

7. Special Conveyances

a. Taxi/Shuttle

A tip not to exceed 15 percent of the cost of the actual taxi/shuttle fare may be claimed as a reimbursable travel expenses. The tip should be added with the cost of the taxi/shuttle when preparing the travel voucher.

b. Rental Automobiles

- i. To ensure usage of a Government-contracted rental vehicle when performing official travel, travelers must reserve and obtain their rental vehicles through the agency Travel Management Service provider.
- ii. In the event of an accident resulting in damage and/or injury, the police must be notified and an accident report must be filed. A copy of the accident report must be provided to the rental car company. In addition, the NIST Safety Office (x5818) must be notified.
- iii. On a case-by-case basis, a request for a larger vehicle may be authorized by the approving official when use of a larger vehicle is officially necessary and justified (e.g., more than two passengers and luggage, transporting Government property, or medically necessary, etc.).
- iv. Usage of Global Positioning Systems (GPS) or maps may be authorized when deemed necessary

in the performance of official travel.

D. Per Diem Expenses

1. Per Diem Allowances

- a. Per diem will not be paid under any circumstances for travel performed that is less than 30 miles from either the employee's official duty station or the employee's residence.
- b. Per diem may be paid within the 30 to 50-mile radius of either the employee's official duty station or the employee's residence when the traveler is attending a conference, training, or if travel conditions are so severe that they would endanger the traveler's safety.
- c. Per diem regulations in the FTR and DOC regulations must be followed for travel greater than 50 miles from either the employee's official duty station or the employee's residence.

2. Lodging

A traveler cannot be reimbursed more for lodging expense than he/she actually incurs.

3. Meals & Incidental Expenses (M&IE)

- a. In limited instances, NIST may allow travelers to claim the full M&IE allowance when they are unable to consume meals furnished by the Government or as part of a conference registration fee (i.e., due to medical requirements or religious beliefs).
- b. If a traveler will be authorized by their approving official to purchase a substitute meal in order to satisfy a medical requirement or religious belief, the travel authorization must include a justification statement. If meal options are not known prior to travel taking place and a meal substitution becomes necessary based on medical requirements or religious beliefs, a post approval will be required on the travel voucher.
- c. Meal allowances should not exceed the applicable M&IE rate for the TDY location unless actual expense was authorized for M&IE.
 - i.
- d. When travel is more than 12 hours, but less than 24 hours, and spans two calendar days, travelers are to be reimbursed 75 percent of the applicable M&IE rate for both calendar days of travel.

4. Reduced Per Diem

- a. Travel assignments lasting more than 30 days are subject to reduced per diem rates.
- b. The per diem rate should be reduced to an amount not less than 55 percent of the applicable per diem rate for the TDY location.

- c. The conditions and necessary costs associated with the extended travel assignment (e.g., living arrangements, ability to cook meals, etc.) are factors to be considered when determining whether the per diem rate should be reduced.
- d. The established reduced per diem rate must be shown on the travel authorization.

5. Actual Expense

- a. Travelers should make every effort to procure suitable lodging/meals within the applicable per diem rate.
- b. When actual expense reimbursement is warranted, it must be approved on the travel authorization.
- c. If circumstances arise while performing official travel that would necessitate actual expense but actual expense was not approved on the original travel authorization, actual expense must be justified and post approved on the travel voucher.
- d. Actual expense will be authorized in accordance with the FTR (Maximum of 300 percent of the applicable per diem rate).

E. Miscellaneous Expenses

1. Miscellaneous Expense Allowances

- a. All miscellaneous expenses must be authorized and approved in accordance with FTR 301-12.
- b. When miscellaneous expenses are authorized by the approving official as necessary in the performance of official business, they will be reimbursed. Authorization of such expenses must be included in the travel authorization.
- c. If circumstances arise while performing official travel that would necessitate miscellaneous expenses that were not approved on the original travel authorization, the miscellaneous expenses must be post approved on the travel voucher.

2. Official Government Passports

- a. NIST was granted a waiver on the use of the CD-97 (Request for Security Assurance and Official Passport Clearance for Foreign Travel) by memo from DOC on July 20, 1998. As a result, travel authorizations must include the date the employee attended the Defensive Travel Briefing, whether or not the embassy will be visited, and contact information for each person to be visited in each country.
- b. Allow 6-8 weeks to process new passport applications or passport renewals.
- c. State Department form DSP-11 is to be used for first-time Government passport applicants.

- d. State Department form DSP-82 is to be used for Government passport application renewals.
- e. Passport applications that are submitted less than 5 weeks from the start date of travel will require an expedite letter. Expedite letters will be drafted by the appropriate administrative staff and must be approved by the OU Director, Deputy Director, or Senior Management Advisor. The approved memo must be submitted to the NIST Travel Office.

3. Travel Visas

- a. The Travel Management Service provider can assist travelers with submission of paperwork for foreign visas; however, each foreign Embassy establishes its own requirements (e.g., cost, processing time, requirements for letters of invitation, etc.) regarding issuance of the visa.
- b. Allow adequate time (6-8 weeks depending upon the country to be visited) for processing visa paperwork.

F. Arranging for Travel Services

- 1. The Travel Management Service provider (Adtrav) must be used for common carrier, lodging and rental car reservations unless you meet one of the exceptions outline in FTR 301-50.8.
- 2. Gaithersburg – For reservations and ticketing assistance, contact the on-site Adtrav Office at x2281. The hours of operation are 8:00 am through 6:00 pm, Monday through Friday (excluding Federal Holidays).
- 3. Boulder – For reservations and ticketing assistance, contact the Adtrav Call Center in Birmingham, AL at 1-866-430-8929.

G. Paying Travel Expenses

1. Government Travel Card

a. Travel Card Issuance

- i. Travel cards may only be issued to Government employees.
- ii. NIST employees who travel 5 or more times per year are required to obtain and use the Government travel card for official travel.
- iii. NIST employees who travel less than 5 times per year are exempt from mandatory use of the Government travel card. On a case-by-case basis, based on mission requirements and individual circumstances, each OU has the discretion to authorize issuance of a travel card to an employee who travels less than 5 times per year. Electronic approval of the travel card application signifies OU authorization.
- iv. Creditworthiness checks will be performed for all employees submitting an application for the Government issued travel card.

- v. Travel card training is mandatory for all cardholders and must be completed every 3 years. A copy of the completed training certificate must be submitted to the Agency/Organization Program Coordinator in the NIST Travel Office at Mailstop 1622.
- b. Travel Card Application
 - i. All travel card applications will be submitted and processed via the PaymentNet website (See section 8.12.07 of this subchapter for additional information).
- c. Travel Card Use
 - i. The Government issued travel card may only be used for official travel expenses. This also includes ATM advances withdrawn for official travel expenses where a credit card is not accepted (taxi, local transportation systems, etc.).
 - ii. All travel card holders are responsible for complying with the terms and conditions of the cardholder agreement.
- d. Travel Card Misuse
 - i. Unauthorized or non-official use of the travel card may result in disciplinary action ranging from reprimand to removal depending upon the circumstances of the misconduct.
 - ii. Written notification will be sent to the cardholder (i.e., traveler), the cardholder's supervisor, and the servicing Human Resources Officer whenever there is a delinquency and/or misuse of the cardholder account. The Office of Inspector General (OIG) may be brought in to investigate where fraud and/or misuse are alleged.
 - iii. Employees who have had their travel card privileges cancelled for misuse will be denied processing of new travel card applications. Travel advances will not be issued for employees who have had their travel card privileges cancelled.
- 2. Travel Advances
 - a. Approved travel advances for NIST employees will be issued by Electronic Funds Transfer (EFT).
 - b. Approved travel advances for invitational and infrequent travelers will be issued by either EFT or Treasury check.
 - c. Only foreign invitational travelers may be issued a convenience check advance.
 - d. After completion of the travel assignment, the outstanding advance issued by EFT, Treasury check or convenience check (foreign only) must be accounted for and applied to the travel claim (See FTR 301-51.202).
 - e. Checks or money orders being submitted to repay an outstanding advance balance should be made payable to DOC/NIST.

H. Claiming Reimbursement

1. Submission of TDY/Long-Term Travel Vouchers

- a. All travel vouchers must be submitted in accordance with chapter 301-52.3 of the FTR and in compliance with the established time frames as listed in chapter 301-52.7.
- b. Travel vouchers for NIST employees are required to be submitted electronically through Travel Manager. A copy of the voucher must be sent to the Travel Office along with all relevant supporting documentation and required receipts.
- c. Travel vouchers for invitational travelers (non-NIST employees) must be submitted in hardcopy form with original signatures in ink. The original voucher must be sent to the Travel Office along with all relevant supporting documentation and required receipts. (See FTR 301-52.4.)

2. Voucher Audits

The following criteria are used to select travel vouchers for internal audit:

- a. All vouchers totaling \$1500.00 or more
- b. Ten percent random sample of vouchers under \$1500.00
- c. All relocations

Note: Occasionally, requests are made by the Department of Commerce, Office of Inspector General, General Services Administration, and/or Congress to review travel documentation meeting the specified data call criteria. In these cases, Personally Identifiable Information is redacted and copies are supplied to the requestor.

I. Using Promotional Materials and Frequent Traveler Programs

Frequent flyer miles obtained in the performance of official travel may be used for future official travel or personal travel. No form CD-334, Request for Approval of Extra- Fare Air Accommodations, is required when upgrading using frequent flyer miles.

J. Collection of Undisputed Delinquent Amounts Owed to the Contract Issuing the Individually Billed Travel Card

See DOC Travel Card policy at <http://www.osec.doc.gov/oas/travel/tchargecard.htm>.

K. Local Travel

1. Local travel does not require a written authorization.
2. Local travel vouchers must be submitted within 30 days after the completion of travel.
3. Employees are required to reach their actual work site and return to their residence at their own

expense. Only travel costs exceeding the normal daily commuting costs will be reimbursed.

4. When employees perform official local travel on a regular work day, only expenses incurred that exceed the normal daily commuting cost will be considered reimbursable.
5. When employees are directed to perform official local travel on a non-work day, expenses incurred will be reimbursed from the authorized starting point of the local travel.

II. Relocation Allowances

A. General Rules

1. Relocation travel cannot be prepared in Travel Manager.
2. Commerce Department forms must be used for the preparation of relocation travel authorizations and vouchers. (See Appendix D.)
3. Relocation travel will be charged to the year in which the relocation travel ensues.
4. Relocation travel vouchers must be submitted in hardcopy form with original signatures in ink. The original voucher(s) must be sent to the Travel Office along with all relevant supporting documentation and required receipts.

B. NIST Payment of Relocation and Travel Expenses for New Hires (Appointees) and Transfers (Transferees)

1. A summary of reimbursable expenses is provided in 5 U.S.C. Sections 5723, 5724, 5724a, 5724b, and 5724c. This information should be used as a guide in determining travel relocation allowances that may be offered under the NIST Alternative Personnel Management System (APMS). For more detailed information regarding travel allowances, please consult the GSA Federal Travel Regulations, 41 CFR Chapter 302, and the Department of Commerce Travel Handbook, Chapter 302.

In addition, the following rules apply:

- a. The vacancy announcement must state whether or not relocation expenses are authorized. Relocation expenses may be authorized when hiring individuals to fill critical shortage positions when included in the job analysis.
- b. When authorized in the vacancy announcement or a critical shortage vacancy:
 - i. Transferring Government employees are reimbursed for all allowances as per their entitlement.
 - ii. New hires (excluding Post Docs) are reimbursed for those allowances that the selecting official, with the approval of the OU Director or the OU Director's designee, has chosen to allow.
 - iii. Post Doctorate Associates are reimbursed for all allowances as per entitlement in FTR 302-3,

Subpart A – New Appointee, Table A. This may also include a househunting trip or temporary quarters subsistence expenses when authorized by the OU Director or the OU Director’s designee. Real estate transactions will not be authorized under any circumstances for Post Doctorate Associates.

- c. All recipients must sign a service agreement (CD-150) indicating commitment of at least 12 months of continuous Government service.
- d. The NIST Travel Office must review all relocation travel orders and subsequent amendments.
- e. Prior to any arrangements being made for movement of household goods, the Traffic Management Officer/Manager must be notified. Gaithersburg must contact NIST Shipping and Receiving in the Administrative Services Division. Boulder must contact the NOAA, Building Management Branch.

Questions regarding travel relocation allowances should be directed to the Travel Office Help Desk on (301) 975-5375 or may be submitted by email to travelof@nist.gov.

C. Transportation of a POV

1. Generally, POV mileage is authorized as most advantageous to the Government when a new hire or transferring employee is traveling from the old official duty station to the new official duty station.
2. Requests for shipment of a POV must be carefully considered and a cost comparison must be completed to determine if the shipment of a POV is cost effective and in the interest of the Government.
3. Although relocation employees may own more than one vehicle, the Government is not required or responsible for the shipment of multiple POVs.
4. If it is determined that shipment of a POV is in the interest of the Government, the maximum weight of the POV and household goods cannot exceed 18,000 pounds. Any weight overages resulting in additional cost will be the responsibility of the traveler.

III. Payment of Expenses Connected with the Death of Certain Employees

A. In the event of death of an employee with pending travel claims, the spouse, child, or other legal representative may sign travel vouchers in lieu of the Claimant.

B. Outstanding amounts due to unused travel advances or audit disallowances are a debt due to the Federal Government. At the appropriate time, the family will be notified of the outstanding balance and the estate will be billed.

IV. Payment of Travel Expenses from A Non-Federal Source

A. Commerce Department forms must be used for the preparation of Gift and Bequest (Assistance-In-Kind) travel. (See NIST Administrative Manual Subchapter 8.10, App. B.)

1. Gift and Bequest Forms

- a. CD 210 – Record of Gift and Bequest
- b. CD-342 – Records of Gifts and Decorations from Foreign Governments

8.12.05

DELEGATIONS OF AUTHORITY

The signature authority and delegation of signature authority for NIST travel authorizations, vouchers, and local travel are as follows:

Domestic	Foreign	Relocation	Local
1) Division Chief OR 2) Signature authority may be delegated to the Group Leader or Administrative Officer.	1) OU Director OR 2) Signature authority may be delegated to the Deputy Director of the OU or the Senior Management Advisor. AND 3) Foreign Travel requires concurrence of the Office of International and Academic Affairs (OIAA).	1) OU Director OR 2) Signature authority may be delegated to the Deputy Director of the OU.	1) Group Leader OR 2) Signature authority may be delegated to the Administrative Officer.

a. The Reviewing Official and Approving Official cannot be the same individual on either the travel authorization or the travel voucher.

b. It is the responsibility of each Operating Unit to provide the Finance Division/Travel Group with a written list of the names of each approving official and his/her designee. The Travel Group will keep the authorized list of approvers on file. In the event of changes or exceptions to a Division's signature authority, the Finance Division/Travel Group must be notified in writing.

8.12.06

RESPONSIBILITIES

- a. Agency (DOC) – The DOC Travel Management Division (TMD) is responsible for maintaining, updating, and issuing new Departmental policies that are pertinent to all Commerce bureaus. In addition, DOC, TMD is responsible for notifying all Commerce bureaus of changes to the DOC policy.
- b. Bureau (NIST) – The Chief Financial Officer, Finance Division, Travel Group is responsible for informing NIST Operating Units of changes to the FTR, CTH, and updates in the NIST Administrative Manual Travel subchapter.
- c. Operating Unit (OU) – NIST Senior Management Advisors and/or Administrative Officers are responsible for disseminating the FTR, CTH, and NIST policy to the appropriate administrative staff, travelers, and approving officials as necessary.

8.12.07

PROCEDURES

- 1. Travel Card
 - a. Training - www.gsa.gov/gasmartpay
 - b. PaymentNet - On-line payments and account access - <https://gov1.paymentnet.com/>
 - c. Application process
 - i. https://www.cc-accountcenter.com/jpmorganchase_commercial/eapp/ss_applicationID.jsp
 - ii. Use DOC73298T as the application ID
- 2. Travel Manager
 - a. Access Travel Manager 9.0 Web. Instructions are available on the usage of the Travel Manager application

8.12.08

CONTENT OWNER

Chief Financial Officer, Finance Division, Travel Group

8.12.09

EFFECTIVE DATE: October 29, 2009

Subchapter 8.12 Official Travel

APPENDIX A

TRAVEL REFERENCES

Listed below are travel and transportation websites that may be accessed to obtain additional travel guidance.

Federal Travel Regulations

<http://www.gsa.gov/Portal/gsa/ep/home.do?tabId=3> *Select Federal Travel Regulations.*

Commerce Travel Handbook

<http://www.osec.doc.gov/oas/travel/default.htm> *Click on Travel Regulations then Commerce Travel Handbook.*

NIST /CFO/Finance/Travel Page

http://www-i.nist.gov/admin/dcfo/finance/travel_group/index.html

Per Diem Rates

Domestic -

http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=17943

Foreign - http://aoprals.state.gov/content.asp?content_id=184&menu_id=78

Oanda (currency conversion rates)

www.oanda.com/convert/classic

Rand McNally (mileage)

<http://www.randmcnally.com/>

Lodging Tax Exemptions -

www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=16366&noc=T

Subchapter 8.12 Official Travel

APPENDIX B

YEAR END TRAVEL PROCESSING

Continuing Resolution

- Per the DOC year-end travel guidance memorandum, the following statement must be annotated on travel orders for the ensuing fiscal year: “Approval of travel scheduled to be accomplished on or after October 1, 20XX (*fill in appropriate year*), is contingent upon the availability of fiscal year 20XX (*fill in appropriate year*) funds.”
- This statement will remain in effect until appropriations have been enacted by Congress and signed into law.

Funding Source

- Per the DOC Office of General Counsel, General Law Division and a passage in the Appropriations Law Red Book (See page 5-15 GAO-04-261SP Appropriations Law-Volume I), no-year funds may be obligated for items that will not materialize until a future fiscal year. (See email from Thomas Klausing, NIST Budget Division, dated August 4, 2005).

Estimated Accruals for Travel

- Due to the immateriality of travel costs, estimated accruals are typically not created for travel expenses.
- If an Expense and Income (E&I) project is being used for the travel expenses, an estimated accrual may be prepared.

Travel Spanning Two Fiscal Years (Split Year Travel)

When no-year funding is not used, travel expenses must be split based on the dates the travel expenses will be incurred.

- Expenses to be incurred on or before September 30, 20XX will be charged to the fiscal year that the travel begins and expenses to be incurred on or after October 1, 20XX will be charged to the fiscal year in which the travel ends.
- The travel authorization must have two valid Accounting Classification Codes (project/task). One for each fiscal year.

Travel for the Ensuing Fiscal Year (New Fiscal Year Travel)

When no-year funding is not used, travel expenses will be charged to the new fiscal year.

Travel authorizations with trip dates beginning on or after October 1, 20XX must have a valid ACCS (project/task) for the applicable fiscal year in which the travel is being performed.

Subchapter 8.12 Official Travel
APPENDIX C

COMMON CARRIER TRANSPORTATION PURCHASES

Requirements for Purchasing Common Carrier Transportation

Form of Common Carrier Transportation Purchase	Action Required
Centrally Billed Account (CBA)	Tickets charged to the centrally billed account require no further action. Common carrier transportation purchased by this method must not be claimed on the travel voucher.
Individually Billed Account – Government Travel Charge Card	<p>When purchased through the Travel Management Service provider (Adtrav), tickets charged to a traveler's individually billed travel card require no further action.</p> <p>Common carrier transportation purchased by this method may be claimed on the travel voucher when authorized.</p> <p>When purchased from a non-Adtrav travel agent or directly from the airline, tickets charged to a traveler's individually billed travel card will require justification on either the travel authorization or a post approval on the travel voucher. Common carrier transportation purchased by this method may be claimed on the travel voucher when authorized.</p>
Personal Credit Card or Cash - (Not Government Card)	<p>Tickets purchased with a personal credit card or cash for less than \$100 require no further action.</p> <p>More than \$100 – A cash exemption memo is required explaining the circumstances that necessitated the purchase of common carrier transportation with cash or a personal credit card.</p>

Subchapter 8.12
APPENDIX D

RELOCATION FORMS

Forms

- CD 29 Travel Order
- CD 150 Request for Authorization of Travel and Moving Expenses
- CD 369 Travel Advance
- CD 370 Travel Voucher
- CD 370A Travel Voucher – Continuation Sheet
- CD 371 Employee Application for Reimbursement of Expenses Incurred Upon Sale
or Purchase (Or Both) of Residence Upon Change of Official Station
- CD 372 Expense Record For Temporary Quarters

HOURS OF DUTY and LEAVE ADMINISTRATION

Sections

10.01.01 Purpose

10.01.02 Scope

10.01.03 Policy

10.01.04 Delegations of Authority for Hours of Duty

10.01.05 NIST Basic Workweek

10.01.06 Official Days and Hours of Duty

10.01.07 NIST Multiple-Shift Schedules

10.01.08 Work at Locations Other Than NIST Premises

10.01.09 First-40-Hours Tour of Duty

10.01.10 Holiday Scheduling

10.01.11 Delegations of Authority for Leave Administration

10.01.12 Leave Documentation Requirements

10.01.13 Administrative Leave

10.01.14 Time Off for Religious Observances

10.01.15 Annual Leave Restoration Procedures

Appendix A - NIST Alternative Work Schedule (AWS) Plan

Appendix C - Special Uses of Sick Leave

10.01.01

PURPOSE

This subchapter states the policies and procedures for NIST employees regarding hours of duty and leave administration.

Subchapter 10.01
Effective date 9/10/04

10.01.02

SCOPE

This subchapter applies to all NIST employees.

10.01.03

POLICY

It is NIST policy to follow the laws and regulations on hours of duty and leave administration as stated in the DoC Handbook on Hours of Duty and Leave Administration (available from the Administrative Officer or the Office of Human Resources Management), the NIST Alternative Work Schedule (AWS) Plan (Appendix A), and the DoC Guidelines for Flexiplace Participation (Appendix B).

It is NIST policy that leave be charged in one-hour increments.

10.01.04

DELEGATIONS OF AUTHORITY FOR HOURS OF DUTY

a. NIST Director -

(1) Authority to establish different official hours of duty other than those listed in Section 10.01.06.

(2) Authority to establish multiple-shift schedules when operations are required to be on a continuous basis (e.g., reactor operations, security, firefighting).

(3) Authority to establish alternative work schedules (AWS).

b. OU Director -

(1) Authority to choose which alternative work schedules will be allowed within each Operating Unit (OU);

(2) Authority to approve standby duty;

(3) Authority to approve hazardous duty;

(4) Authority to establish first-40-hours tour of duty; and

(5) Authority to approve flexiplace participation.

The Office of Human Resources Management (OHRM) should be consulted when it is anticipated that authorities listed above are to be exercised since supervisors need to be

Subchapter 10.01

Effective date 9/10/04

informed regarding pay entitlements and timekeeping.

10.01.05

NIST BASIC WORKWEEK

NIST has established for full-time employees a basic workweek of 40 hours. The basic workweek shall be scheduled during a period of five consecutive days from Monday through Friday of each week. Under the NIST Alternative Work Schedule (AWS) Plan (Appendix A), other workweeks are permitted. Employees on a first-40-hours tour of duty have a basic workweek defined as "a period of not more than six days of an administrative workweek consisting of seven consecutive calendar days."

10.01.06

OFFICIAL DAYS AND HOURS OF DUTY

The official days and hours of the NIST locations are:

- a. Gaithersburg and all Field Offices (except Boulder) - 8:30 a.m. to 5:00 p.m., Sunday through Saturday, with 30 minutes for lunch to be taken between 11:30 a.m. and 1:30 p.m., except for those employees on alternative work schedules.
- b. Boulder - 8:00 a.m. to 5:00 p.m., Sunday through Saturday, with 1 hour for lunch to be taken between 11:30 a.m. and 1:30 p.m., except for those employees on alternative work schedules.

10.01.07

NIST MULTIPLE-SHIFT SCHEDULES

- a. Definition - Multiple-shift schedules occur when operations are required to be on a continuous basis (e.g., reactor operations, security, firefighting).
- b. Considerations -
 - (1) When multiple-shift schedules are required, any two consecutive days in the basic workweek may be designated as regularly scheduled days off.
 - (2) Supervisors may assign employees to the various approved shifts on the basis of the needs of the operation.
 - (3) The memorandum to the NIST Director requesting a multiple-shift schedule should state when the lunch period is to be taken.

10.01.08

WORK AT LOCATIONS OTHER THAN NIST PREMISES

Each employee is required to perform official duties on NIST premises except:

Subchapter 10.01

Effective date 9/10/04

- a. As otherwise required by the specific nature of the duties, including performance of duty while in a travel status and performance in an approved training assignment and approved by appropriate OU management.
- b. NIST policy permits employment at the employee's home in accordance with existing laws, regulations, and DoC Guidelines for Flexiplace Participation (Appendix B). In these situations, approval in advance is required by the OU Director.
- c. When an employee is detailed to another agency or international organization.
- d. When the official duty station is other than NIST premises.

10.01.09

FIRST-40-HOURS TOUR OF DUTY

- a. The first-40-hours tour of duty is performed within a period of not more than six days of an administrative workweek consisting of seven consecutive calendar days. This tour may be established as the basic workweek for certain full-time employees when all of the following exist: (1) the nature of the work is the paramount consideration; (2) it is determined a definite schedule of regular hours of work would seriously impair the accomplishment of the work to be performed; (3) it is determined that a schedule of regular hours would result in substantial increase in costs of operation; (4) the work is such that it cannot be accomplished within the regular tour of duty through a temporary adjustment of hours or approval of overtime; and (5) an alternative work schedule including maxiflex, would not accommodate the organization's needs. First-40-hours tours of duty are approved by the OU Director and renewed on an annual basis.
- b. At least one day each administrative workweek must be considered a non-workday.
- c. Except when a holiday occurs within the administrative workweek, first-40-hour employees must work a total of 40 hours or a charge to leave or LWOP will be made for the difference. For example, first-40-hour employees will be given credit for 8 hours for a holiday towards their 40 hours minimum work requirement and they need not work on that day. [Proportionate credit will be given when a holiday is less than a full day.]
- d. Time used for the following activities is not creditable for purposes of meeting the first-40-hours requirement:
 - (1) Unauthorized work performed at home or other unofficial location.
 - (2) Official travel away from the official duty station scheduled to occur within the Monday through Friday, 40-hour workweek of the office or employee (Section 16 of PL-89-301).
- e. Sunday through Saturday is designated as the administrative workweek for employees with this type of tour.

Subchapter 10.01

Effective date 9/10/04

- f. Considerations prior to approval should include: (a) the safety and security of the employee during working hours; (b) the supervision of the employee during working hours; (c) the pay entitlements of the employee (e.g., night differential); and (d) accountability for timekeeping. These considerations should be addressed in the written request to the OU Director for approval.
- g. Employees are expected to return to their regular tour of duty when the work does not require a first-40-hour tour. A first-40-hours tour of duty is not established primarily for the convenience of an employee.
- h. Requests for approval must be submitted in writing from the requesting official to the OU Director. A Standard Form (SF) 52, Request for Personnel Action, must accompany the written request. After approval by the OU Director, the request package must be submitted to the OHRM for review and processing.
- i. The same rules for earning, requesting, and approving leave that apply to employees having a regularly scheduled workweek also apply to first-40-hour employees. Leave may be taken during NIST regular working hours (Monday-Friday).
- j. To protect an employee with respect to employee compensation (for injury) and other fringe benefits and to facilitate the resolution of questions which may arise in connection with tort claims against the government, supervisors of employees who have a first-40-hour basic workweek shall, insofar as practicable, predetermine for the employee concerned the specific times when the employee is expected to be in a duty status.

10.01.10

HOLIDAY SCHEDULING

- a. General Rules - When a holiday falls on a workday, that work day is the holiday. When a holiday falls on a Saturday, the day that is treated as the holiday is the preceding Friday. When a holiday falls on a Sunday the day that is treated as the holiday is the subsequent Monday.
- b. For Employees on Compressed Work Schedules - When a day that is treated as the holiday falls on an employee's scheduled day off (i.e., a non-workday), the day to be treated as the holiday is the workday immediately before the scheduled day off, EXCEPT when the day that is treated as the holiday falls on a Monday, and that is the employee's scheduled day off, then the day that is treated as the holiday is the subsequent workday. For example, if the holiday falls on a Saturday, the day to be treated as the holiday is the preceding Friday. However, if that Friday is an employee's scheduled day off (i.e., a non-workday) the day to be treated as the holiday is the preceding Thursday. If the holiday falls on a Sunday, the day to be treated as the holiday is the following Monday. However, if that Monday is an employee's scheduled day off (i.e., a non-workday) the day to be treated as the holiday is the following Tuesday.

An employee on a compressed work schedule is paid for the number of hours normally worked the day on which the holiday falls.

Subchapter 10.01

Effective date 9/10/04

c. For Employees on Maxiflex, Variable Day, or Variable Workweek Schedules - An employee on a Maxiflex, Variable Day, or Variable Week work schedule gets the holiday if it falls on a workday. If the holiday does not fall on a workday the day to be treated as the holiday is their workday immediately before the holiday. Employees on these flexible work schedules may not be paid more than 8 hours for a holiday they do not work. Part-time employees must be paid for the holiday on a prorated basis in accordance with their work schedule.

d. For Employees on First-40-Hours - If the holiday falls on a Saturday and Saturday is a non-workday, the day to be treated as a holiday is the workday immediately before the holiday. If the holiday falls on a Sunday and Sunday is a non-workday, the day to be treated as the holiday is the subsequent workday. If a holiday falls on a workday that day shall be treated as the holiday, and the employee's basic 40-hour tour of duty shall be deemed to include eight hours on that day.

10.01.11

DELEGATIONS OF AUTHORITY FOR LEAVE ADMINISTRATION

a. The NIST Deputy Director has authority to approve the following in addition to those authorized in b., c., and d. below:

(1) Restoration of leave when requestor is OU Director.

(2) Administrative leave for site-wide closing (e.g., weather, equipment failure, etc.) or early dismissal beyond one hour directly preceding a holiday (e.g., Christmas Eve).

b. The OU Director has authority to approve the following in addition to those authorized in c. and d. below:

(1) Leave restoration for exigency of business.

(2) Leave-without-pay (LWOP) when retention of annual leave is requested.

(3) Administrative leave beyond one hour (except blood donation which is delegated to the first-level supervisor).

c. Division chief (or equivalent) has authority to approve the following in addition to those authorized in d. below:

(1) LWOP of more than 30 days when retention of annual leave is not requested;

(2) Advanced sick leave (This authority is delegated to the first-level supervisor in all OUs except 810);

(3) LWOP up to 30 days when retention of annual leave is not requested (This authority is delegated to the first-level supervisor in all OUs except 830); and

Subchapter 10.01

Effective date 9/10/04

(4) Annual leave, sick leave or LWOP requested under the Family and Medical Leave Act (FMLA). (This authority is delegated to the first-level supervisor in all OUs except 810, 830, and 860.).

d. First-level supervisor has authority to approve:

(1) Annual leave (for personal use for all OUs);

(2) Advanced annual leave;

(3) Sick leave {for personal use, Federal Employees Family Friendly Leave Act (FEFFLA), or PL-103-329 for all OUs);

(4) Advanced sick leave (except OU 810 where this authority is retained by the division chief);

(5) Administrative leave up to one hour;

(6) Administrative leave up to four hours for blood donation;

(7) Military leave;

(8) Court leave;

(9) LWOP, for personal use, up to 30 days when retention of annual leave is not requested (except OU 830 where this authority is retained by the division chief);

(10) Annual leave, sick leave or LWOP requested under the FMLA (except OUs 810, 830, and 860 where this authority is retained by the division chief);

(11) Leave restoration for administrative error, sickness, or injury; and

(12) Leave transfer.

10.01.12

LEAVE DOCUMENTATION REQUIREMENTS

Leave documentation is to be retained within the OU as part of time and attendance records for six years.

a. Annual Leave - Annual leave is for personal use or for use as a substitute for LWOP under the FMLA. Annual leave is coded as 61 on the Form CD-440, Time and Attendance Report.

(1) Accrued - SF-71, Application for Leave, the employee's initials on Form CD-440 (whichever is required by the supervisor) with the first-level supervisor's certifying

Subchapter 10.01

Effective date 9/10/04

signature on Form CD-440. If accrued annual leave is requested as a substitute for LWOP under the FMLA, see below.

(2) Advanced - SF-71 completed by employee and approved by the first-level supervisor. The SF-71 should be annotated to show "advanced annual leave."

(3) FMLA -

(a) Form CD-518, Application for Family and Medical Leave (in lieu of the SF-71) completed by the employee and approved by the leave approving official.

(b) If annual leave is requested for more than three consecutive days to care for a family member, an acceptable certificate signed by a physician or other practitioner or other written evidence acceptable to the leave approving official. The Remarks section of Form CD-440 is annotated with "___ hours FMLA." The timekeeper must also keep a record of the total hours of annual leave used under the FMLA within a 12-month period so that the employee does not exceed the 12-week limitation.

b. Sick Leave - Sick leave is for personal use (i.e., illness, doctor, or dental appointments), for use under the FEFFLA, for use under PL-103-329, or for use as a substitute for LWOP under the FMLA. Sick leave is coded as 62 on Form CD-440, except for FEFFLA which is coded prefix 62/TC62.

(1) Accrued - (for personal, FEFFLA, or PL-103-329)

(a) SF-71 or the employee's initials on Form CD-440 (whichever is required by the supervisor) with the first-level supervisor's certifying signature on Form CD-440. If sick leave is requested as a substitute for LWOP under the FMLA, see below.

(b) If sick leave requested is for more than three consecutive days, an acceptable certificate signed by a physician or other practitioner or other written evidence acceptable to the supervisor.

(c) If sick leave requested is for adoption purposes under PL-103-329, legal adoption papers or letters which verify adoption proceedings are required in addition to the documents listed above.

(d) If the sick leave is requested under either the FEFFLA or PL-103-329, the Remarks section of Form CD-440 must be annotated as " hours" for (either FEFFLA or PL-103-329). The timekeeper must keep a record of the total hours of sick leave used for these purposes so that the employee does not exceed the limitations stated within the FEFFLA or PL-103-329.

(2) Advanced - (for personal, FEFFLA, or PL 103-329)

Subchapter 10.01

Effective date 9/10/04

(a) SF-71 completed by the employee and approved by the leave approving official. The SF-71 should be annotated to show, "advanced sick leave."

(b) An acceptable medical certificate signed by a physician or other practitioner or other written evidence acceptable to the leave approving official.

(c) If advanced sick leave is requested for adoption purposes under PL-103-329, legal adoption papers or letters that verify adoption proceedings in addition to the documents listed above.

(3) FMLA -

(a) Form CD-518 (in lieu of the SF-71) completed by the employee and approved by the leave approving official. The Remarks section of Form CD-440 is annotated with " hours FMLA." The timekeeper must keep a record of the total hours of sick leave used under the FMLA within a 12-month period so that the employee does not exceed the 12-week limitation.

(b) If sick leave requested is for more than three consecutive days, an acceptable certificate signed by a physician or other practitioner or other written evidence acceptable to the leave approving official.

c. Leave-Without-Pay (LWOP) - LWOP may be used in lieu of annual or sick leave for personal use or for use under the FMLA. All LWOP is coded as 71 on Form CD-440. NOTE: Use of LWOP may affect an employee's health benefits, life insurance coverage, leave accrual, service computation date, career tenure, and completion of probationary period.

(1) 30 Calendar Days or Less -

(a) SF-71 completed by the employee and approved by the leave approving official. If retention of annual leave is requested, state the number of hours on the SF-71. If LWOP is requested under the FMLA, see below.

(b) If LWOP supplements sick leave for a total of more than three consecutive days for personal use or to care for a family member under the FMLA, an acceptable medical certificate signed by a physician or other practitioner or other written evidence acceptable to the leave approving official (if not previously obtained).

(2) More than 30 Calendar Days -

(a) SF-71 completed by the employee and approved by the leave approving official. If retention of annual leave is requested, state the number of hours on the SF-71. If LWOP is requested under the FMLA, see below.

Subchapter 10.01

Effective date 9/10/04

(b) An SF-52, Request for Personnel Action, for LWOP must be submitted to the servicing personnel generalist along with a copy of the approved SF-71.

(c) If LWOP supplements sick leave for a total of more than three consecutive days for personal use or to care for a family member under the FMLA an acceptable medical certificate signed by a physician or other practitioner or other written evidence acceptable to the leave approving official (if not previously obtained).

(3) FMLA -

(a) Form CD-518 (in lieu of SF-71) completed by the employee and approved by the leave approving official. The Remarks section of Form CD-440 annotated with " hours FMLA." The timekeeper must keep a record of the total hours of LWOP used under the FMLA within a 12-month period so that the employee does not exceed the 12-week limitation.

(b) If LWOP supplements sick leave for a total of more than three consecutive days to care for a family member, an acceptable certificate signed by a physician or other practitioner or other written evidence acceptable to the leave approving official (if not previously obtained).

d. Military Leave - Military leave is an approved absence from duty, with pay, authorized for employees who are members of the National Guard or reserve components of the Armed Forces, for days which they are ordered to active duty. Military Leave is coded as 65 on Form CD-440.

(1) SF-71 completed by the employee and approved by the first-level supervisor.

(2) A copy of authorized military orders.

e. Court Leave - Court leave is an approved absence from official duties, without loss of or reduction in pay or leave to perform jury duty or to serve as a witness, in a non-official capacity for the federal government or a state or local government. Court leave is coded as 66 on Form CD-440.

(1) SF-71 completed by the employee and approved by the first-level supervisor.

(2) A copy of an official court order to perform jury duty or serve as a witness.

f. Leave Transfer -

(1) Leave Recipient - Form CD-504, Recipient's Leave Share Application, completed by the employee and approved by the supervisor.

(2) Leave Donor (within DoC) - Form CD-505, Donor's Leave Transfer Application, completed by the employee and approved by the first-level supervisor.

Subchapter 10.01

Effective date 9/10/04

(3) Leave Donor (outside DoC) - Form OPM-630B, Request to Donate Leave to Leave Recipient, under the Leave Transfer Program, completed by the employee and approved by the first-level supervisor.

10.01.13

ADMINISTRATIVE LEAVE

Administrative leave is excused absence with pay and may be granted under certain conditions noted in Section II of the DoC Handbook on Hours of Duty and Leave Administration. Employees granted administrative leave as a result of an early dismissal must be in a work status at the time the dismissal is announced to receive the administrative leave. Employees in a travel status do not receive administrative leave as a result of an early dismissal. Refer to Subchapter 6.02 for specific NIST policies regarding delayed arrival, late opening, and early closing. Administrative leave is coded as 66 on Form CD-440.

10.01.14

TIME OFF FOR RELIGIOUS OBSERVANCES

When personal religious beliefs require that an employee abstain from work during certain periods of the workday or workweek, the employee may, in lieu of annual leave or leave without pay, request, earn and take compensatory time as authorized in DAO 202-554, Premium Pay, Section 8. Compensatory time is requested and authorized using Form CD-81, Authorization for Paid Overtime and/or Holiday Work, and for Compensatory Overtime.

10.01.15

ANNUAL LEAVE RESTORATION PROCEDURES

a. Documentation Requirements - The following documentation must be submitted to the appropriate OU approving official:

(1) Administrative Error -

(a) SF-71 approved by the first-level supervisor.

(b) Form CD-479, Request for Restoration of Annual Leave, approved by the first-level supervisor explaining in detail the nature of the error, when the error occurred, when the error was made known to the employee, and the reason for not rescheduling the leave.

(c) Form CD-527, Audit for Leave Year ____, for the year in which the leave was forfeited.

(2) Sickness or Injury -

(a) SF-71 approved by the first-level supervisor.

Subchapter 10.01

Effective date 9/10/04

(b) Form CD-479 approved by the supervisor explaining in detail the nature of the sickness or injury and the reason for not rescheduling the leave that was forfeited.

(c) Form CD-527 for the year in which the leave was forfeited.

(3) Exigency of Business -

(a) SF-71 approved by the first-level supervisor.

(b) Form CD-479 approved by first-level supervisor and OU Director explaining in detail the nature of the exigency and the reason for not rescheduling the forfeited leave.

(c) Form CD-527 for the year in which the leave was forfeited.

b. Instructions for Completion of Form CD-479 -

(1) Year Leave was Forfeited - Provide leave year.

(2) Basis of Request - Check one.

(3) Hours Forfeited - Hours to be forfeited at end of leave year, if restoration is not approved.

(4) Hours Requested for Restoration - Cannot exceed the number of hours to be forfeited.

(5) Employee's Name - Provide name.

(6) Title, Series, Grade - Provide title, series, and grade/pay band.

(7) Organization - Organizational unit name and number.

(8) Reason for the Request - State specific details for the request and why leave could not be rescheduled. Attach Form CD-527, signed and dated, and SF-71.

(9) From and To - Dates of each instance of scheduled annual leave cancelled to be restored.

(10) Number of Hours - Number of hours for each instance of scheduled annual leave cancelled and to be restored.

(11) Date of Approval - Date of approval on SF-71 for each instance of scheduled annual leave.

(12) Date of Cancellation - Leave blank.

Subchapter 10.01

Effective date 9/10/04

(13) Proposed Schedule for Use of Restored Leave - From and To - Date(s) and time(s) for proposed use of restored leave.

(14) Leave Restored the Previous Year - Number of hours restored, basis for restoration and number of hours used to date.

(15) Immediate Supervisor - Signature, title, and date.

(16) Reviewing Official - The reviewing official is the second-level supervisor as required by the OU.

(17) Servicing Personnel Officer - N/A.

(18) Approving Official - Appropriate OU approving official signature, title, and date.

When annual leave is approved for restoration under any of the conditions above all original documentation is retained in the Time and Attendance file of the employee. A copy of Form CD-479 is provided to the leave approving official, the employee, and Payroll/Processing (OHRM) at Gaithersburg or the Chief, Systems Operations Branch at Boulder.

APPENDIX A

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MARYLAND
AND
BOULDER, COLORADO**

**Alternate Work Schedule (AWS) Plan
(Under DAO 202-610)**

A. Organizational Units Covered. With the exceptions noted in the second paragraph, this plan for AWS covers all employees of the National Institute of Standards and Technology (NIST), Gaithersburg and Boulder.

B. Coverage Exceptions. Except for the following, all employees may participate in this AWS plan; however, employees are not required to participate. Employees not participating in AWS will remain on the regular fixed schedule: 8:30 a.m. to 5:00 p.m. for Gaithersburg and 8:00 a.m. to 5:00 p.m. for Boulder (Boulder has a one-hour non-paid lunch period). Exceptions are (1) employees on intermittent, shift, or first 40 schedules, (2) employees when on TDY or in particular situations while in training status and (3) all NIST employees represented by the following unions:

1. International Association of Firefighters
2. International Association of Machinists and Aerospace Workers, Local 174
3. Washington Area Metal Trades Council
4. AGE Local 2186

The Operating Unit (OU) Directors may exclude specific organizational elements from participation if the function cannot be covered adequately.

C. Work schedules Permitted. The following alternatives are available for use by employees, with management approval at the OU Director level and division level. The use of these alternatives by an employee must be approved by his/her first-line supervisor and Division Chief, in order to ensure mission effectiveness, internal productivity, organizational efficiency, and personal safety.

1. Four-day work week - This alternative allows a full-time employee to work four days a week, 10 hours each day for a total of 40 hours per week, 80 hours per pay period. Part-time employees are also eligible for this work schedule. A part-time employee may be scheduled to work fewer than 40 hours a week in fewer than five work days. All employee's scheduled tour must be between 7:00 a.m. and 7:00 p.m. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

2. **5/4-9** - This alternative allows a full-time employee to work a pay period of eight nine-hour days and one eight-hour day, with one day off, in whatever order agreed upon. Part-time employees may be scheduled to work fewer than 80 hours a biweekly pay period in fewer than 10 days. All employee's scheduled tour must be between 7:00 a.m. and 7:00 p.m. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

3. **Flexitour** is a flexible schedule in which an employee, having once selected starting and stopping times within the flexible time bands, continues to adhere to these times. Occasional changes to the schedules may be made with the supervisor's approval in advance. Full-time employees may request to begin their day any time between 7:00 a.m. and 9:30 a.m. and to end their day any time between 3:30 p.m. and 7:00 p.m., provided a minimum of eight hours is worked. Part-time employees should work one-half of their tour within core hours. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

4. **Gliding schedule** is a flexible schedule in which a full-time employee has a basic work requirement of eight hours in each day and 40 hours in each week, and may select an arrival time each day and may change that arrival time daily, without supervisory approval, as long as it is within the established flexible time band. Part-time employees should work one-half of their tour within core hours. All employee's tour must be between 7:00 a.m. and 7:00 p.m. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

5. **Variable Day** is a schedule in which an employee works a flexible work schedule containing core hours on **each workday** in the week and in which an employee has a basic work requirements of 40 hours in each week of the biweekly pay period, but in which an employee may vary the number of hours worked on a given workday within the week within the limits established for NIST/OU/Division. Part-time employees must work 16 hours in a week. A variable day is not subject to the 7:00 a.m. and 7:00 p.m. time bands except that the core hours must be worked each work day. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

6. **Variable Week** is a schedule in which an employee works a flexible week schedule containing core hours on **each workday** in the biweekly pay period in which an employee has a basic work requirement of 80 hours for the biweekly pay period, but in which an employee may vary the number of hours worked on a given workday or the number of hours each week within the limits established for NIST/OU/Division. Part-time employees must work 32 hours within a biweekly pay period. Variable week is not subject to 7:00 a.m. and 7:00 p.m time bands, except that the core hours must be worked each work day. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

7. **Maxiflex** is a schedule in which an employee works a flexible work schedule that contains core hours on **fewer** than 10 work days in the biweekly pay period and in which

Subchapter 10.01

Effective date 9/10/04

an employee has a basic work requirement of 80 hours for the biweekly pay period (or multiple thereof), but in which an employee may vary the number of hours worked on a given workday or the number of hours each week within the limits established for NIST/OU/Division. Maxiflex is not subject to the 7:00 a.m. and 7:00 p.m. time bands. Once adopted, change from this alternative can be made only with approval at the same level as the original approval.

D. Core Hours and Flexible Time Bands (MAXIFLEX is an exception.)

7:00 a.m. - 9:30 a.m. Flexible Band

9:30 a.m. - 11:30 a.m. Core Hours

11:30 a.m. - 1:30 p.m. Flexible Band

1:30 p.m. - 3:30 p.m. Core Hours

3:30 p.m. - 7:00 p.m. Flexible Band

On those days when an employee is in a duty status, he/she must be on duty during core hours or absences must be charged to leave, compensatory time, or leave without pay (Maxiflex is an exception). Lunch time (noncompensable, minimum of 1/2 hour) may be scheduled anytime between 11:30 a.m. and 1:00 p.m. in order to be completed by 1:30 p.m., and is required for any day's schedule of more than five hours. Part-time employees should work at least half of their schedule during core hours.

An approval of any of the above alternatives must be consistent with mission effectiveness, internal productivity, organizational efficiency, and personal safety.

E. GAO Approved Time Accounting Systems. Supervisors must select one, or a combination, of the following time accounting systems or techniques:

1. Serial sign-in/sign-out sheets using the CD-465. Signing in and out must be done chronologically in the order of arrival and departure.
2. Face-to-face oversight. Supervision will be provided for all hours employees work. Arrivals and departures will be physically observed. Supervisors will make a written record on the official T&A of any deviations from approved schedules.
3. Arrangements with other supervisory personnel to provide observation.
4. Occasional supervisory telephone calls to the employee during times the supervisor is not present but the employee is scheduled to work.
5. Occasional observation by the supervisor through the supervisor coming to work earlier or staying later than the supervisor's scheduled tour.
6. Determining reasonableness of work output for time spent.

The supervisor officially is responsible for employee attendance and accuracy of time attendance reports, as well as investigating any time-reporting discrepancies and initiating disciplinary action when violations or abuses are evident.

F. Primary Consideration/Final Approval and Revocation of Approval. A critical consideration in approval and continuance of any of these alternative schedules for individual employees will be continued mission effectiveness, internal productivity, organizational efficiency and personal safety. Thus, sufficient kinds of numbers of employees must be present to carry out operations efficiently and effectively. With this consideration in mind, all AWS must be approved by the Division Chief and can be revoked by the Division Chief. The requests must flow through the first line supervisor to the Division Chief.

G. Administration and Evaluation. The Director of NIST is responsible for the overall efficient functioning of this plan. The OU Director is responsible for deciding which AWS are offered within the OU. Division Chiefs are responsible for the day-to-day administration of the plan. The Personnel Officer will submit all necessary reports to higher agency levels.

Evaluation of the plan and reporting results will be ongoing and will occur at least annually. Evaluation will cover adherence to the provisions of the plan, mission effectiveness, internal productivity, and organizational efficiency. Evaluation also would cover problems that arose and what was done about them, as well as what worked well. Additionally, the Director of NIST will evaluate the plan in terms of the provisions, adequacy of coverage, and efficiency of operation.

H. Organizational Modification/Termination. Modifications may be recommended at any time by supervisors or employees, making such recommendations to the Director of NIST~in writing. The Director will decide whether or not to adopt any recommendations, subject to DoC approval. In general, major modifications, when adopted, will not be made except at the beginning of the next calendar year. The Director may terminate participation in this plan for all or part of the total organization at any time. Any terminations will be based on the findings of the evaluation process, on adherence to plan provisions, mission effectiveness, internal productivity, and organizational efficiency.

APPENDIX C

SPECIAL USES OF SICK LEAVE

Federal Employees Family Friendly Leave Act (FEFFLA)

On October 22, 1994, Congress enacted the Federal Employees Family Friendly Leave Act, (FEFFLA), Public Law 103-388. This Act was effective on December 2, 1994. The Act expands the use of sick leave for purposes of: (1) providing care for a family member as a result of physical or mental illness; injury; pregnancy; childbirth; or medical, dental, or optical examination or treatment; or (2) making arrangements necessitated by the death of a family member or attending the funeral of a family member. A "family member" under this Act is defined as a spouse and his or her parents; children, including adopted, foster or step children, and their spouses; parents; brothers and sisters, and their spouses; and any individual related by blood or affinity, whose close personal relationship with the employee is the equivalent of a family member. Under the FEFFLA, full-time employees are able to use an initial total of up to 40 hours of sick leave for family care or funeral-related purposes. Full-time employees who maintain a balance of 80 hours of sick leave may use an additional 64 hours of sick leave for these purposes, for an authorized total of 104 hours within a leave year. Part-time employees may also use sick leave for these purposes in amounts prorated to the number of hours worked weekly.

Public Law 103-329

Effective September 30, 1994, the Treasury, Postal Service and General Government Appropriations Act for FY 95, Public Law 103-329, authorizes sick leave to be used for purposes of adoption of a child. Although this legislation was enacted on September 30, 1994, the provisions are retroactive to September 30, 1991. Therefore, employees who have used annual leave for adoption purposes between September 30, 1991, and September 30, 1994, were entitled to request that sick leave be substituted for all or a portion of the annual leave used. This Act also entitles employees up to seven days of administrative leave in a calendar year for time necessary to serve as a bone-marrow or organ donor.

Documentation

Leave approving officials should request documentation from employees (e.g., medical certification, obituary, etc.) consistent with current leave approving procedures for sick leave or leave-without-pay. The leave approving official and the timekeeper must ensure that the leave used is properly coded and that a remark indicating the purpose (e.g., FEFFLA, adoption, etc.) is placed in the Remarks section of Form CD-440. Timekeepers should assist the leave approving official with monitoring leave used for purposes authorized under these Acts by keeping a running total of the number of hours used in the Remarks Section of Form CD-440.

Subchapter 10.08

Dated: 5-20-05

TRAINING

Sections

10.08.01 Purpose

10.08.02 Scope

10.08.03 Policy

10.08.04 Definitions

10.08.05 Roles and Responsibilities

10.08.06 Continuous Learning

10.08.07 Individual Development Plan

10.08.08 Probationary Supervisors

10.08.09 Failure to Complete a Course

10.08.10 Membership in Professional Organizations

10.08.11 Professional Credentials

10.08.12 Continued Service Agreement

10.08.13 Academic Degrees

10.08.14 Approval Criteria

10.08.15 Data Collection

Subchapter 10.08

Dated: 5-20-05

10.08.01

PURPOSE

This subchapter sets forth the National Institute of Standards and Technology (NIST) policy and procedures for the training program, following the laws, regulations, and policies listed below.

1. 5 United States Code, Chapter 41
2. 5 CFR, Chapter 410.101
3. Guidance on Public Law 104-52
4. Executive Order 11348
5. OPM Training Policy Handbook: www.opm.gov/leader/hrd/lead/policy/flex.asp
6. Merit Systems Principles, Title 5 U.S. Code Chapter 23, 2301(b)

10.08.02

SCOPE

This subchapter applies to all NIST employees at Gaithersburg and Boulder.

10.08.03

POLICY

It is NIST policy to train and develop NIST employees for maximum achievement of goals and objectives in accordance with applicable laws and regulations noted above.

10.08.04

DEFINITIONS

a. Training – The process of providing for and making available to an employee and placing or enrolling the employee in a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education in scientific, professional, technical, mechanical, trade, clerical, fiscal, administrative, or other field which will improve individual and organizational performance and assist in achieving the agency's mission and performance goals.

b. Mission-Related Training – Training that supports agency goals by improving organizational performance at any appropriate level in the agency, including training that:

- (1) Supports the agency's strategic plan and performance objectives;
- (2) Improves an employee's current job performance;
- (3) Allows for expansion or enhancement of an employee's current job;
- (4) Enables an employee to perform needed or potentially needed duties outside the current job at the same level of responsibility; or
- (5) Meets organizational needs in response to human resource plans and engineering, downsizing, restructuring, and/or program changes.

Subchapter 10.08

Dated: 5-20-05

10.08.05

ROLES AND RESPONSIBILITIES

The authority to approve training for all NIST employees is delegated to the Operating Unit (OU) level. The OU Director may delegate the approval authority to the Division Chief, but no lower than the Division Chief.

Supervisors are responsible for ensuring that courses are completed by discussing the outcome of the course with the employee, by requesting a transcript from the employee, or by any other appropriate means.

10.08.06

CONTINUOUS LEARNING

Continuous learning is a necessary ingredient for the staff of any organization that strives for continuous improvement and values technical, managerial, and administrative excellence in its work. A formal policy that addresses continuous learning provides a guideline for supervisors and staff to plan learning activities that all staff should be participating in for the pursuit of improving their ability to accomplish their work. Learning can be done through the following:

- (1) Courses in academic institutions;
- (2) Internal and external training sessions (includes management and leadership programs, and other on-the-job training required by NIST management);
- (3) Seminars and courses that help employees develop a better understanding of their fellow employees and how to conduct oneself as a Federal employee (i.e., diversity, ethics, safety);
- (4) Developmental assignments; and
- (5) Information training such as technical sessions of two hours or more at a professional or technical society meeting.

The NIST Deputy Director establishes a target for the average number of hours of continuous learning to be taken by the staff within each Operating Unit.

Operating Unit Directors must ensure that each employee's performance plan includes requirements for continuous learning to be tracked by the supervisor. Staff (both supervisors and non-supervisors) may take up to half of their continuous learning activities in information training. Supervisors must take at least half of their continuous learning in leadership/management type activities. Developmental assignments are to be considered as fulfilling the yearly requirement for an employee.

10.08.07

INDIVIDUAL DEVELOPMENT PLAN

An Individual Development Plan (IDP) is a document that identifies an individual's

Subchapter 10.08

Dated: 5-20-05

learning and development goals. The employee and supervisor prepare it jointly. It contains training, education, work assignments, and formal and informal activities to acquire skills and competencies for both current job and future career growth. The IDP is at the supervisor's discretion.

- a. Benefits – NIST must invest in the development of its human resources to meet demands of the future. Creating an IDP serves as a commitment between NIST and the employee to work towards specific goals, provides a mechanism to communicate those goals, and provides greater assurance that career development will be a success. It provides another way for supervisors to learn of the interests of the employee and for the employee to learn about current and future needs of NIST and other opportunities.
- b. Responsibilities – Employees are responsible for their careers and for identifying their developmental goals and opportunities. Supervisors are responsible for assisting employees through career guidance discussions and for identifying opportunities consistent with individual and NIST objectives.
- c. Process – The employee prepares for a career guidance discussion by identifying professional and career goals, skills that need further development, and knowledge and experiences that seem to be important for growth in the chosen career field. The supervisor prepares by considering the activities that may be beneficial for the employee and potential opportunities considering NIST's current needs and future directions. The employee and the supervisor have a career guidance discussion and document the developmental goals and activities. NIST Document Number (DN) 13 is available for use. The employee and supervisor monitor and review progress on the IDP on a semi-annual basis.

10.08.08

PROBATIONARY SUPERVISORS

Probationary supervisors are required to complete the Management Survival Skills training course prior to the one-year anniversary date of appointment.

10.08.09

FAILURE TO COMPLETE A COURSE

If an employee fails or does not complete a course, or resigns from NIST prior to completion of a course, it is the employee's responsibility to inform the supervisor of such. The supervisor uses their discretion to determine whether to request the employee to reimburse the government. If an employee is terminated from NIST prior to completion of a course, the employee is not obligated to reimburse the government.

10.08.10

MEMBERSHIP IN PROFESSIONAL ORGANIZATIONS

The law prohibits using appropriated funds to pay for individual employee memberships in professional associations and societies. There are, however, several ways for NIST to

Subchapter 10.08

Dated: 5-20-05

obtain the professional, scientific, and technical information that associations provide their members. Two examples are described below:

(1) Association membership is often included in registration fees for a conference or meeting. If NIST pays the registration fees, the employee's membership in the association is considered an incidental by-product of meeting attendance.

(2) NIST may purchase an organizational membership in an association or society. NIST may also purchase a membership for a specific position, such as the position of Medical Director. The incumbent in that position uses membership to improve the conduct, supervision, or management of his or her function.

10.08.11

PROFESSIONAL CREDENTIALS

The Defense Authorization Act for FY 2002, codified in 5 U.S.C. 5757, allows agencies to use appropriated funds or funds otherwise available to the agency to pay expenses for employees to obtain professional credentials, including expenses for professional accreditation.

This authority allows NIST the flexibility to pay for licenses and credentials that relate to the mission, goals, and objectives of the agency. Use of this authority must be applied consistent with merit system principles. Paying for credentials is at the discretion of the approving official.

10.08.12

CONTINUED SERVICE AGREEMENT

An employee selected for a training course (over 80 hours) must agree in writing within their OU and prior to the training assignment, that they will continue in the service of NIST after the end of the training period for a time at least equal to three times the length of the training period.

If the employee departs NIST before the agreed upon amount of service has occurred, the agency has the right to require repayment for the amount of time not served. The approving official may waive in whole or in part a right of recovery if it is shown that the recovery would be against equity and good conscience or against the public interest.

10.08.13

ACADEMIC DEGREES

The law (Title 5, United States Code, Chapter 41, 4107(a) and (b)) does not authorize the approval of training for an academic degree unless it is necessary to assist in the recruitment or retention of employees in occupations in which the government has or anticipates a shortage of qualified personnel, especially in occupations involving critical skills. The law does not authorize the approval of training for the purpose of an academic degree to qualify for an appointment to a particular position for which the degree is a basic requirement.

Subchapter 10.08

Dated: 5-20-05

10.08.14

APPROVAL CRITERIA

Training may be approved when it meets the definition of training or mission-related training in Section 10.08.04 above and when it is in accordance with Merit System Principles listed below:

- (1) Recruit qualified individuals from all segments of society and select and advance employees on the basis of merit after fair and open competition;
- (2) Treat employees and applicants fairly and equitably, without regard to political affiliation, race, color, religion, national origin, sex, marital status, age, or handicapping condition;
- (3) Provide equal pay for equal work and reward excellent performance;
- (4) Maintain high standards of integrity, conduct, and concern for the public interest;
- (5) Manage high standards of integrity, conduct, and concern for the public interest;
- (6) Manage employees efficiently and effectively;
- (7) Retain or separate employees on the basis of their performance;
- (8) Educate and train employees when it will result in better organizational or individual performance;
- (9) Protect employees from improper political influence; and
- (10) Protect employees against reprisal for the lawful disclosure of information in "whistle blower" situations (i.e., protect people who report things such as illegal and/or wasteful activities).

Training can be approved using the following mechanisms, government bankcard, SF-182, Request, Authorization, Agreement and Certification and the DN-11, Request for Training Memo. Forms are available on the Administration Online Forms Page, and E-Approval. The DN-11 is used for all internal training and when training is put on the government bankcard. The SF-182 is used when a vendor will not accept the government bankcard or the dollar amount exceeds the amount authorized for the government bankcard.

10.08.15

DATA COLLECTION

Each Organizational Unit (OU) is responsible for maintaining data for all mandatory training and probationary supervisory training. This data should be entered into the continuous learning database.

TIME AND ATTENDANCE

Sections

10.17.01 Purpose

10.17.02 Scope

10.17.03 Legal Authority

10.17.04 Policy

10.17.05 Delegations of Authority

10.17.06 Definitions

10.17.07 Responsibilities

10.17.08 Enforcement

10.17.09 Procedures

10.17.10 Content Owner

10.17.11 Effective Date

10.17.01

PURPOSE

This subchapter outlines the procedures for Time and Attendance at the National Institute of Standards and Technology.

10.17.02

SCOPE

This subchapter applies to all NIST employees.

10.17.03

LEGAL AUTHORITY

Departmental policy and procedures for time and attendance are required and authorized by United States General Accounting Office GAO-03-352G (formerly Title 6 of the General Accountability Office's Policy and Procedures Manual for Guidance to Federal Agencies).

10.17.04

POLICY

Subchapter 10.17

Dated: 08/05/09

It is NIST policy to follow Departmental policy and procedures as stated in the DoC Time and Attendance Manual (available with T&A Liaisons, timekeepers, and in the NIST Human Resources Management Division) and Human Resources (HR) Bulletins #FY06-032 and FY07-064.

10.17.05

DELEGATIONS OF AUTHORITY

Pursuant to DoC policy, the supervisory responsibilities for reviewing, approving, and certifying time and attendance data may not be re-delegated to non-supervisory personnel.

10.17.06

DEFINITIONS

Supervisor is defined as an employee whose official position description includes “Supervisory Responsibilities” wherein the employee performs full range of supervision over one or more employees in performance appraisal, leave administration, and EEO.

WebTA is a web-based time and attendance software application that is currently used to record, validate, certify, and submit time and attendance data (hours worked and leave taken) to the Department’s payroll/personnel service provider, the National Finance Center (NFC), for salary payment.

10.17.07

RESPONSIBILITIES

Various individuals at different organizational levels, including employees, timekeepers, supervisors, Time & Attendance Contact Points, Time & Attendance Liaisons, Human Resources personnel (DoC and NIST) are involved in the biweekly timekeeping process. The individual roles and their respective responsibilities are outlined in the Departmental policy referenced in 10.17.04.

10.17.08

ENFORCEMENT

The immediate consequence of non-compliance is a possible delay in salary payments to affected employees. The long-term consequences for not complying with established policy and internal controls include the possibility of waste, fraud, and/or abuse. Employees who fail to comply with time and attendance policy and procedures may be subject to disciplinary action up to and including removal from the Federal service.

10.17.09

PROCEDURES

It is NIST policy to follow Departmental procedures for time and attendance, which are available online at the DoC website under the heading “webTA.” Procedures referenced online include webTA Guides by user role, webTA transaction codes, and webTA Validation Messages.

10.17.10

CONTENT OWNER

Human Resources Management Division

Subchapter 10.17

Dated: 08/05/09

10.17.11

EFFECTIVE DATE

August 5, 2009

IONIZING RADIATION SAFETY

Sections

12.03.01 Purpose

12.03.02 Background

12.03.03 Scope

12.03.04 Legal Authority

12.03.05 Policy

12.03.06 Delegation of Authority

12.03.07 Definitions

12.03.08 Acronyms

12.03.09 Responsibilities

12.03.10 Enforcement

12.03.11 Content Owner

12.03.12 Effective Date

12.03.13 References

12.03.01

PURPOSE

The purpose of this subchapter is to describe the NIST Gaithersburg and Boulder ionizing radiation safety programs and the radiation safety responsibilities of NIST employees and non-NIST personnel (i.e., associates and contractors).

12.03.02

BACKGROUND

a. Radiation Safety Programs

- (1) NIST implements an ionizing radiation safety program at the NIST Gaithersburg site (“Gaithersburg radiation safety program”) in accordance with Nuclear Regulatory Commission (NRC) Materials License Number SNM-362, Exempt Quantity Distribution License Number 19-

23545-01E, and Test Reactor License Number TR-5 and applicable Federal, State, and local regulations. The program has two functional areas: Radiation Facilities (e.g., those facilities containing radioactive materials, and ionizing-radiation-producing devices) and the Reactor Facility at the NIST Center for Neutron Research (NCNR)

(2) NIST also implements an ionizing radiation safety program at the NIST Boulder site (“Boulder radiation safety program”) in accordance with NRC Materials License Number 05-03166-05 and applicable Federal, State, and local regulations. The program has one functional area which encompasses facilities containing radioactive materials and ionizing-radiation-producing devices.

b. Radiation Safety Committees

(1) The Ionizing Radiation Safety Committee (IRSC) assists the NIST Director in the oversight of the operations and activities of NIST’s radiation safety programs except for those operations and activities conducted under the NRC Test Reactor License, as described in NIST Administrative Manual Subchapter 3.01, Appendix A. The IRSC reports to the NIST Director.

(2) The Safety Evaluation Committee (SEC) has oversight of the operations and activities conducted under the NRC Test Reactor License, as described in the TR-5 license document. The SEC reports to the Director of the NIST Center for Neutron Research.

(3) The Safety Assessment Committee (SAC) provides a broad spectrum of expertise in reactor technology, as described in the TR-5 license document. The SAC reports to the Director of the NIST Center for Neutron Research.

12.03.03

SCOPE

a. The provisions of this subchapter apply to:

- (1) All NIST employees and non-NIST personnel assigned to the NIST Gaithersburg and Boulder sites;
- (2) The on-site and off-site locations where NIST-owned or controlled ionizing radiation sources are utilized;
- (3) The acquisition, use, transfer, and disposal of ionizing radiation sources under the purview of the NRC licenses held by NIST;
- (4) The acquisition, use, transfer, and disposal of NRC generally-licensed and exempt-quantity ionizing radiation sources; and
- (5) The acquisition, use, and transfer of ionizing-radiation-producing devices.

12.03.04

LEGAL AUTHORITY

a. NRC License Numbers SNM-362, 19-23545-01E, 05-03166-05, and TR-5 (which includes Technical Specifications).

12.03.05

POLICY

It is NIST policy that the exposure of individuals, members of the public, and the environment to ionizing radiation shall be kept As Low As Reasonably Achievable (ALARA) and in compliance with the terms and conditions specified in NRC licenses and applicable Federal, State, and local regulations.

12.03.06

DELEGATION OF AUTHORITY

The NIST Director hereby delegates to the CSO, the IRSC, and the Gaithersburg and Boulder RSOs the authority necessary to carry out their responsibilities. The NIST Director delegates to the IRSC and to the Gaithersburg and Boulder RSOs the authority to stop immediately any operations that may (1) compromise the safety or health of NIST employees and non-NIST personnel; (2) have an adverse impact on the public or environment; or (3) result in non-compliance with NRC, State, or local requirements.

12.03.07

DEFINITIONS

Because of significant differences between NIST's radiation safety programs in Gaithersburg and Boulder, some definitions pertain to only one site.

a. As Low As Reasonably Achievable (ALARA) – The lowest achievable level of radiation exposure and release of radioactive material when taking into account the state of technology, the economics of precautions in relation to benefits, and the beneficial utilization of atomic and nuclear energy.

b. Authorized User – An individual at NIST Boulder whose training and experience have been reviewed and approved by the NIST Boulder RSO, the IRSC, and, if necessary, the NRC, and who has been authorized by Management to use and directly supervise the use of radioactive material at NIST Boulder.

c. Byproduct Material –

(1) Any radioactive material (except special nuclear material) yielded in, or made radioactive by, exposure to radiation incident to the process of producing or using special nuclear material;

(2) Any material that has been made radioactive by use of a particle accelerator, and is produced, extracted, or converted after extraction for use in a commercial, medical, or research activity; or

(3) Any discrete source of naturally occurring radioactive material, other than source material, that the NRC, in consultation with the Administrator of the Environmental Protection Agency, the Secretary of Energy, the Secretary of Homeland Security, and the head of any other appropriate Federal agency, determines would pose a threat similar to the threat posed by a discrete source of

radium-226 to the public health and safety or the common defense and security, and is extracted or converted after extraction for use in a commercial, medical, or research activity.

d. Exempt Quantity – An individual quantity of byproduct material, which does not exceed the applicable quantity set forth in 10 CFR 30.71, Schedule B and which is not listed on any NRC license (Specific or Broad Scope) currently held by NIST. No person may, for purposes of producing an increased amount of radioactivity or radiation level, combine quantities of byproduct material covered by this exemption so that the aggregate quantity exceeds the limits set forth in 10 CFR 30.71, Schedule B.

e. General License – A license provided by regulation that grants authority to a person for certain activities involving byproduct material and is effective without the filing of an application with the NRC or the issuance of a licensing document to a particular person. A general license permits an individual to acquire, receive, possess, use, and transfer byproduct material contained in devices designed and manufactured for the purpose of detecting, measuring, gauging, or controlling thickness, density, level, interface location, radiation, leakage, or qualitative or quantitative chemical composition, or for producing light or an ionized atmosphere.

f. Health Physics (HP) Group – The group of technical and administrative staff members at NIST Gaithersburg that supports the Gaithersburg RSO.

g. Health Physics Instructions (HPIs) – The set of procedures approved by the Gaithersburg RSO and implemented by the HP Group in support of the SNM-362 and 19-23545-01E NRC Licenses.

h. Radiation Safety Instructions (RSIs) – The set of documents approved by the Boulder RSO that implement the NIST ionizing radiation safety policies for ionizing radiation sources used by NIST personnel on the Boulder campus.

i. Ionizing Radiation – Alpha particles, beta particles, gamma rays, x-rays, neutrons, high-energy electrons, high-energy protons, and other particles capable of producing ions when they impinge on, or penetrate matter, hereinafter often referred to as radiation.

j. Ionizing Radiation Sources – Radioactive materials, including generally-licensed sources, exempt-quantity sources, and irradiators, and ionizing-radiation-producing devices.

k. Ionizing-Radiation-Producing Devices – Devices that generate ionizing radiation when energized, including, but not limited to, X-ray units, particle accelerators, neutron generators, and electron microscopes.

l. Management – An Organizational Unit (OU) Director or the Director of the NIST Boulder Laboratories, or an individual who has been delegated the authority to make decisions on that person's behalf.

m. NCNR User – An individual who utilizes the neutron beam lines, pneumatic transfer system, or any laboratory/room containing ionizing radiation sources at the NCNR.

- n. NIST-364 – The NIST form entitled “Radioactive Material Request” that documents the request and approval process required by the NIST Gaithersburg RSO for the acquisition and use of radioactive material, and for Source User(s) and use and storage locations.
- o. NIST-365 – The NIST form entitled “Change to Radioactive Material Request” that documents the request and approval process required by the NIST Gaithersburg RSO for changes in the utilization of radioactive material, or in the Source Custodian, Source User(s), or use and storage locations.
- p. NIST/BL-100 – The NIST Boulder form entitled “Boulder Radioactive Material Request” that documents the request and approval process required by the NIST Boulder RSO for the acquisition and use of radioactive material, and for Authorized User(s), Supervised User(s), and use and storage locations.
- q. NIST/BL-101 – The NIST Boulder form entitled “Change to Boulder Radioactive Material Request” that documents the request and approval process required by the NIST Boulder RSO for changes in the utilization of radioactive material, or in the Authorized User(s), Supervised User(s), or use and storage locations.
- r. Occupational Dose – Dose received by an individual in the course of employment in which the individual’s assigned duties involve exposure to radiation or to ionizing radiation sources from licensed and unlicensed sources of radiation, whether in the possession of the licensee or other person. Occupational dose does not include doses received from background radiation, from medical procedures, from exposure to individuals administered radioactive material, from voluntary participation in medical research programs, or as a member of the public.
- s. Radiation Facility – A building, room, or area, excluding those under the purview of the TR-5 license, which has been approved in writing by the RSO or designee and authorized by Management for the purpose of using or storing ionizing radiation sources.
- t. Radiation Facilities Group Leader – The individual who oversees the implementation of the radiation safety and ALARA programs at NIST Gaithersburg Radiation Facilities.
- u. Radiation Facility Owner – An individual authorized by Management to maintain and manage access to a Radiation Facility.
- v. Radiation Facility User – Any individual authorized by Management to have unescorted access to a Radiation Facility.
- w. Radiation-Safety Significant – A hazard assessment result that indicates a potential for adverse safety and health or regulatory compliance issues, as identified by the RSO, or designee.
- x. Reactor Facility Group Leader – The individual who oversees the implementation of the radiation safety and ALARA programs at NIST Gaithersburg Reactor Facility.
- y. Reactor Operator – An individual licensed by the NRC to manipulate the controls of the NBSR.

z. Radiation Safety Officer – An individual who is responsible for managing a radiation safety program and all aspects of the utilization of ionizing radiation sources under that program in compliance with the terms and conditions specified in applicable Federal, State, and local regulations.

aa. Radioactive Material Package Receiver – An individual who accepts a radioactive material package from a common carrier for delivery to the HP Group in Gaithersburg or the RSO in Boulder.

bb. Source Custodian – An individual at NIST Gaithersburg approved in writing by the NIST Gaithersburg RSO or designee and authorized by Management to materially control, use, or otherwise manipulate ionizing radiation sources and to be responsible for the primary control and accountability of ionizing radiation sources.

cc. Source Material –

(1) Uranium or thorium or any combination of uranium and thorium in any physical or chemical form; or

(2) Ores that contain, by weight, one-twentieth of 1 percent (0.05 percent), or more, of uranium, thorium, or any combination of uranium and thorium. Source material does not include special nuclear material.

dd. Source User – An individual at NIST Gaithersburg approved in writing by the NIST Gaithersburg RSO or designee and authorized by Management to materially control, use, or otherwise manipulate ionizing radiation sources.

ee. Special Nuclear Material –

(1) Plutonium, uranium-233, uranium enriched in the isotope 233 or in the isotope 235, and any other material that the NRC determines to be special nuclear material, but not including source material; or

(2) Any material artificially enriched by any of the foregoing but not including source material.

ff. Supervised User – An individual at NIST Boulder approved in writing by the NIST Boulder RSO and IRSC and authorized by Management to materially control, use, or otherwise manipulate ionizing radiation sources but only under the direct observation of an Authorized User.

gg. Ionizing-Radiation-Producing Device User – An individual approved in writing by the RSO or designee and, in the case of Boulder, by the IRSC, and authorized by Management to materially control, use, or otherwise manipulate an ionizing-radiation-producing device.

12.03.08

ACRONYMS

a. ALARA – As Low As Reasonably Achievable.

b. CSO – Chief Safety Officer.

- c. HP – Health Physics.
- d. HPI – Health Physics Instruction.
- e. RSI – Radiation Safety Instruction.
- f. IRSC – Ionizing Radiation Safety Committee.
- g. NCNR – NIST Center for Neutron Research.
- h. NRC – Nuclear Regulatory Commission.
- i. OU – Organizational Unit.
- j. RSO – Radiation Safety Officer.
- k. SAC – Safety Assessment Committee.
- l. SEC – Safety Evaluation Committee.

12.03.09

RESPONSIBILITIES

a. The NIST Director is responsible for:

- (1) Ensuring the implementation of ionizing radiation safety programs at NIST that conform to the ionizing radiation safety policy in Section 12.03.05;
- (2) Appointing all IRSC members, subject to NRC license requirements;
- (3) Approving changes to the IRSC charter, subject to NRC license requirements;
- (4) Providing direction to the CSO and IRSC, as necessary;
- (5) Reviewing IRSC recommendations and directing action on those recommendations as necessary to ensure radiation safety and regulatory compliance;
- (6) Ensuring proper allocation of resources to satisfy safety and regulatory requirements;
- (7) Ensuring the implementation of accountability and enforcement policies in support of safety and regulatory compliance; and
- (8) Providing direction on significant issues involving worker safety, regulatory compliance, and environmental impacts at the NIST Gaithersburg and Boulder sites.

c. The CSO is responsible for:

(1) Overseeing the establishment, implementation, and maintenance of ionizing radiation safety programs at NIST, exclusive of the program supporting the TR-5 license, that conform to the ionizing radiation safety policy in Section 12.03.05;

(2) Serving as the Content Owner for this subchapter in accordance with the requirements of NIST Administrative Manual Subchapter 4.01; and

(3) Submitting applications for renewals of and amendments to NRC License Numbers SNM-362, 19-23545-01E, and 05-03166-05 pursuant to IRSC review and approval.

d. The IRSC assists the NIST Director in the oversight of the operations and activities of NIST's radiation safety programs except for those operations and activities conducted under the TR-5 license. The IRSC is responsible for:

(1) Recommending actions to the NIST Director as necessary to ensure radiation safety and regulatory compliance;

(2) Reporting to the NIST Director at least annually on the status of the ionizing radiation safety program (at intervals not to exceed fifteen (15) months);

(3) Approving or rejecting requests made using the NIST-364 form for the acquisition and use of radioactive material at NIST Gaithersburg, including Source Users, Source Custodian, and use and storage locations, when the NIST Gaithersburg RSO or designee has determined that such requests are radiation-safety significant;

(4) Approving or rejecting requests made using the NIST-365 form for changes in the use of radioactive material at NIST Gaithersburg, or in Source Custodian, Source Users, or use and storage locations, when the NIST Gaithersburg RSO or designee has determined that such requests are radiation-safety significant;

(5) Approving or rejecting requests for the acquisition and use of ionizing-radiation-producing devices at NIST Gaithersburg, including Ionizing-Radiation-Producing Device Users and use locations, when the NIST Gaithersburg RSO or designee has determined that such requests are radiation-safety significant;

(6) Approving or rejecting requests for changes in the use of ionizing-radiation-producing devices at NIST Gaithersburg, or in Ionizing-Radiation-Producing Device Users or use locations, when the NIST Gaithersburg RSO or designee has determined that such requests are radiation-safety significant;

(7) Approving or rejecting requests made using the NIST/BL-100 form for the acquisition and use of radioactive material at NIST Boulder, including Authorized Users, Supervised Users, and use and storage locations;

- (8) Approving or rejecting requests made using the NIST/BL-101 form for changes in the use of radioactive material at NIST Boulder, or in Authorized Users, Supervised Users, or use and storage locations;
- (9) Approving or rejecting requests for the acquisition and use of ionizing-radiation-producing devices at NIST Boulder, including Ionizing-Radiation-Producing Device Users and use locations;
- (10) Approving or rejecting requests for changes in the use of ionizing-radiation-producing devices at NIST Boulder, or in Ionizing-Radiation-Producing Device Users or use locations;
- (11) Approving or rejecting proposed applications for license amendment to NIST Gaithersburg NRC licenses SNM-362 or 19-23545-01E and NIST Boulder NRC license 05-03166-05;
- (12) For NRC licenses SNM-362, 19-23545-01E, and 05-03166-05, reviewing Applications for License Amendment, responses to Requests for Additional Information, Licensee Event Reports, and responses to Notices of Violation for completeness and accuracy;
- (13) Reviewing the circumstances of all reportable occurrences, identifying root causes and contributing factors, recommending to the NIST Director measures to preclude a recurrence, and tracking actions on those recommendations as needed;
- (14) Reviewing the circumstances of incidents and violations of NIST radiation safety program requirements when the RSO has determined that they are radiation-safety significant and tracking actions resulting from such reviews as needed; and
- (15) Carrying out the additional specific duties listed in the IRSC Charter.

e. The NIST SEC has responsibility for evaluating and reviewing nuclear safety associated with the operation and use of the NBSR and for carrying out the functions described in the TR-5 license.

f. The NIST SAC has responsibility for reviewing NCNR reactor operations and the performance of the SEC and for carrying out the functions described in the TR-5 license.

g. The NIST Gaithersburg RSO is responsible for managing the radiation safety program and all aspects of the utilization of ionizing radiation sources at NIST Gaithersburg in support of NRC License Numbers SNM-362 and 19-23545-01E. These responsibilities include:

- (1) Establishing and maintaining an effective radiation safety program that allows for the safe and regulatorily compliant use of ionizing radiation sources in a manner that conforms to the NIST policy;
- (2) Establishing and maintaining a system for hazard analysis, mitigation planning, and emergency response planning integrated into ionizing radiation source use protocols and Radiation Facility authorizations;
- (3) Approving or rejecting, or designating a member of the HP Group to approve or reject, requests made using the NIST-364 form for the acquisition and use of radioactive material, including

Source Users, Source Custodian, and use and storage locations; determining whether such requests are radiation-safety significant, and if so, transmitting those requests to the IRSC for approval or rejection;

(4) Approving or rejecting, or designating a member of the HP Group to approve or reject, requests made using the NIST-365 form for changes in the utilization of radioactive material, or in Source Custodian, Source Users, or use and storage locations; determining whether such requests are radiation-safety significant, and if so, transmitting those requests to the IRSC for approval or rejection;

(5) Approving or rejecting, or designating a member of the HP Group to approve or reject, requests for the acquisition and use of ionizing-radiation-producing devices, including Ionizing-Radiation-Producing Device Users and use locations; determining whether such requests are radiation-safety significant, and if so, transmitting those requests to the IRSC for approval or rejection;

(6) Approving or rejecting, or designating a member of the HP Group to approve or reject, requests for changes in the utilization of ionizing-radiation-producing devices, or in Ionizing-Radiation-Producing Device Users or use locations; determining whether such requests are radiation-safety significant, and if so, transmitting those requests to the IRSC for approval or rejection;

(7) Providing advice and assistance on radiological safety matters to individuals whose assigned duties involve the use of or exposure to ionizing radiation sources and working closely with the IRSC and NIST executive management in implementing the radiation safety program;

(8) Identifying radiation safety issues and initiating, recommending, providing, and verifying implementation of corrective actions;

(9) Assisting the IRSC in the performance of its duties, including providing timely information to the IRSC on issues and incidents with potentially significant adverse impact on radiation safety or regulatory compliance;

(10) Documenting and reporting metrics indicating the status of the radiation safety program to the IRSC, NIST management, and regulators as required;

(11) Evaluating reports of radiation hazards and reporting evaluation results that imply the existence of defects or items of non-compliance with NRC regulations to the Chair of the IRSC, within 24 hours of receiving such reports;

(12) Establishing and updating guidance, procedures, instructions, and other requirements to promote radiation safety and regulatory compliance;

(13) Providing radiation safety training to those who require it commensurate with duties;

(14) Maintaining records of radiation safety training and ensuring individuals are notified when refresher training is due; and

(15) Maintaining records of source acquisition, utilization, transfers, and disposal.

h. The NIST Gaithersburg HP Group is responsible for providing support to the NIST Gaithersburg RSO in the management of the radiation safety program and utilization of ionizing radiation sources at NIST Gaithersburg in support of NRC License Numbers SNM-362, 19-23545-01E, and TR-5 (which includes Technical Specifications). These responsibilities include:

(1) Complying with the requirements of the NIST HPIs; and

(2) Identifying to the Radiation Facilities Group Leader or Reactor Facility Group Leader, whichever is applicable, any issues that have, or may have, radiological safety concerns or regulatory compliance implications.

i. The NIST Boulder RSO is responsible for managing the radiation safety program and all aspects of the utilization of ionizing radiation sources at NIST Boulder in support of NRC License Number 05-03166-05. These responsibilities include:

(1) Establishing and maintaining an effective radiation safety program that allows for the safe and regulatorily compliant use of all ionizing radiation sources in a manner that conforms to the NIST policy;

(2) Establishing and maintaining a system for hazard analysis, mitigation planning, and emergency response planning integrated into ionizing radiation source use protocols and Radiation Facility authorizations;

(3) Approving or rejecting, and transmitting to the IRSC for its approval or rejection, requests made using the NIST/BL-100 form for the acquisition and use of radioactive material, including Authorized User(s), Supervised User(s), and use and storage locations;

(4) Approving or rejecting, and transmitting to the IRSC for its approval or rejection, requests made using the NIST/BL-101 form for changes in the utilization of radioactive material, or in Authorized User(s), Supervised User(s), or use and storage locations;

(5) Approving or rejecting, and transmitting to the IRSC for its approval or rejection, requests for the acquisition and use of ionizing-radiation-producing devices, including Ionizing-Radiation-Producing Device Users and use locations;

(6) Approving or rejecting, and transmitting to the IRSC for its approval or rejection, requests for changes in the utilization of ionizing-radiation-producing devices, or in Ionizing-Radiation-Producing Device Users or use locations;

(7) Providing advice and assistance on radiological safety matters to individuals whose assigned duties involve the use of or exposure to ionizing radiation sources and working closely with the IRSC and NIST executive management in implementing the NIST Boulder radiation safety program;

(8) Identifying radiation safety issues and initiating, recommending, providing, and verifying implementation of corrective actions;

- (9) Assisting the IRSC in the performance of its duties, including providing timely information to the IRSC on issues and incidents with potentially significant adverse impact on radiation safety or regulatory compliance;
- (10) Documenting and reporting metrics indicating the status of the radiation safety program to the IRSC, NIST management, and regulators as required;
- (11) Evaluating reports of radiation hazards and reporting evaluation results that imply the existence of defects or non-compliances with NRC regulations to the Chair of the IRSC, within 24 hours of receiving such reports;
- (12) Establishing and updating guidance, procedures, instructions, and other requirements to promote radiation safety and regulatory compliance;
- (13) Serving as back up to Authorized Users to assure control and accountability for sources whenever the Authorized User is unable to fulfill those duties;
- (14) Providing radiation safety training to those who require it commensurate with duties;
- (15) Maintaining records of radiation safety training and ensuring individuals are notified when refresher training is due; and
- (16) Maintaining records of source acquisition, utilization, transfers, and disposal.

j. The Director of the NCNR is responsible for matters involving the Reactor Facility and the TR-5 license, including:

- (1) Adhering to all requirements of the TR-5 License and Technical Specifications;
- (2) Reporting to the NRC on defects and items of noncompliance with NRC regulations for matters dealing with the Reactor Facility;
- (3) Ensuring appropriate radiation safety and ALARA practices are implemented within the areas covered by the TR-5 license; and
- (4) Minimizing exposure of the general public and facility personnel to radiation resulting from reactor operations.

k. NIST OU Directors and the Director of the NIST Boulder Laboratories are responsible for:

- (1) Ensuring that NIST employees and non-NIST personnel (where applicable) in their areas of responsibility comply with the requirements of this subchapter and OU-specific radiation safety requirements;
- (2) Ensuring that appropriate hazard assessments have been performed, hazards mitigation plans are implemented prior to the commencement of work, and emergency response plans are

incorporated into research protocols and procedures involving the use of ionizing radiation sources in accordance with the requirements of: this subchapter and of NIST Administrative Manual Subchapter 12.06, Hazard Analysis and Control;

(3) Authorizing the acquisition and use of radioactive materials, Source User(s), Source Custodian(s), Authorized User(s), Supervised User(s), use location(s), and storage location(s), and changes in same, subject to the requirements of NIST-364, NIST-365, NIST/BL-100, and NIST/BL-101 forms, as applicable, pursuant to approval by the RSO or designee in Gaithersburg or the RSO in Boulder;

(4) Authorizing Radiation Facilities and Ionizing-Radiation-Producing Device Users pursuant to approval by the RSO or designee;

(5) Authorizing Radiation Facility Owners and Radiation Facility Users;

(6) Providing programs that utilize ionizing radiation sources with the proper resources and facilities to ensure compliance with the radiation safety programs that implement the requirements of NRC License Numbers SNM-362, 19-23545-01E , and 05-03166-05;

(7) Ensuring control and accountability for sources when Source Custodians are unable to fulfill their duties; and

(8) Implementing ionizing radiation source accountability and enforcement policies in support of safety and regulatory compliance.

OU Directors and the Director of the NIST Boulder Laboratories may delegate the authority to carry out their responsibilities to others, but the responsibilities remain solely theirs.

l. Gaithersburg Division Chiefs are responsible for:

(1) Approving or rejecting requests made using the NIST-364 form for the acquisition and use of radioactive material, Source User(s), Source Custodian, and use and storage locations;

(2) Approving or rejecting requests made using the NIST-365 form for changes in the utilization of radioactive material, or in Source Custodian(s), Source User(s), or use and storage locations;

(3) Identifying to their OU Director and the Gaithersburg RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;

(4) Completing radiation safety training on the control of and accountability for ionizing radiation sources; and

(5) Supporting Radiation Facility Owners in managing the access to, and security of, their assigned facilities.

m. Gaithersburg Group Leaders are responsible for:

- (1) Approving or rejecting requests made using the NIST-364 form for the acquisition and use of radioactive material, Source User(s), Source Custodian, and use and storage locations;
- (2) Approving or rejecting requests made using the NIST-365 form for changes in the utilization of radioactive material, or in Source Custodian(s), Source User(s), or use and storage locations; ensuring coordination with the former Source Custodian, if applicable;
- (3) Identifying to their Division Chief and the Gaithersburg RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;
- (4) Completing radiation safety training on the control of and accountability for ionizing radiation sources; and
- (5) Supporting Radiation Facility Owners in managing the access to, and security of, their assigned facilities.

n. Boulder Division Chiefs are responsible for:

- (1) Approving or rejecting requests made using the NIST/BL-100 form for the acquisition and use of radioactive material, Authorized User(s), Supervised User(s), and use and storage locations;
- (2) Approving or rejecting requests made using the NIST/BL-101 form for changes in the utilization of radioactive material, or in Authorized User(s), Supervised User(s), or use and storage locations;
- (3) Identifying to their OU Director, the Director of the NIST Boulder Laboratories, and the Boulder RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;
- (4) Completing radiation safety training on the control of and accountability for ionizing radiation sources; and
- (5) Supporting Radiation Facility Owners in managing the access to, and security of, their assigned facilities.

o. Boulder Group Leaders are responsible for:

- (1) Approving or rejecting requests made using the NIST/BL-100 form for the acquisition and use of radioactive material, Authorized User(s), Supervised User(s), and use and storage locations;
- (2) Approving or rejecting requests made using the NIST/BL-101 form for changes in the utilization of radioactive material, or in Authorized User(s), Supervised User(s), or use and storage locations;
- (3) Identifying to their Division Chief and the Boulder RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;

- (4) Completing radiation safety training on the control of and accountability for ionizing radiation sources; and
- (5) Supporting Radiation Facility Owners in managing the access to, and security of, their assigned facilities.

p. The Radiation Facilities Group Leader is responsible for:

- (1) Supporting the implementation of the radiation safety and ALARA programs at NIST Gaithersburg in support of the SNM-362 and 19-23545-01E licenses, and in accordance with the NIST Gaithersburg HPIs; and
- (2) Conducting the appropriate surveillance activities and reporting radiological issues concerning the SNM-362 and 19-23545-01E licenses to the NIST Gaithersburg RSO.

q. The Reactor Facility Group Leader is responsible for:

- (1) Supporting the implementation of the radiation safety and ALARA programs at the Reactor Facility in support of the TR-5 license using the guidelines of the American National Standard for Radiation Protection at Research Reactor Facilities (ANSI/ANS 15.11-2004), and in accordance with the requirements of SNM-362 license and the NIST Gaithersburg HPIs;
- (2) Conducting the appropriate surveillance activities and reporting radiological issues concerning the Reactor Facility and TR-5 license to the Director of the NCNR;
- (3) Advising the NIST Gaithersburg RSO on radiological matters concerning the Reactor Facility and the TR-5 license; and
- (4) Conducting the appropriate surveillance activities and reporting radiological issues concerning the Reactor Facility in regard to the SNM-362 license to the NIST Gaithersburg RSO.

r. Radiation Facility Owners are responsible for:

- (1) Maintaining a list of Radiation Facility Users having authorized access to their assigned facilities;
- (2) Managing the access to, and security of, their assigned facilities;
- (3) Completing the required training for the types of hazards associated with their assigned facilities, and with the ionizing radiation sources used or stored in their facilities;
- (4) Identifying to their supervisor and the appropriate RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;
- (5) Ensuring that procedures and engineering controls are used to keep occupational doses and doses to members of the public ALARA; and

(6) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

s. Radiation Facility Users are responsible for:

- (1) Only entering Radiation Facilities unescorted when they have been authorized by Management to do so;
- (2) Completing all training required by the NIST radiation safety program, including training on the safe use of ionizing radiation sources; maintaining the security of, and access to, ionizing radiation sources; and recognizing and responding appropriately to incidents involving ionizing radiation sources to prevent the spread of contamination;
- (3) Controlling access to, and maintaining the security of, Radiation Facilities while occupying such facilities;
- (4) Complying with the requirements of occupying a Radiation Facility;
- (5) Identifying to the respective Radiation Facility Owner, Source Custodian (if applicable), and the appropriate RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications; and
- (6) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

t. Source Custodians are responsible for:

- (1) Making their sources available for use only to approved and authorized Source Users;
- (2) Completing, as part of requests made using NIST-364 and NIST-365 forms, the appropriate hazard assessments and establishing the hazard mitigation and emergency response plans, if applicable, for their ionizing radiation sources through coordination with the HP Group;
- (3) Ensuring prior to any use of a source that Source Users are informed of the terms and conditions specified in the NIST-364 form and associated documents, and in any applicable NIST-365 forms, specific to the use of the source, including use protocols and hazard mitigation and emergency response plans;
- (4) When appropriate, initiating requests using the NIST-365 form for changes in the utilization of radioactive material, or in Source User(s) or use and storage locations;
- (5) Completing all training required by the NIST radiation safety program, including training on the safe use of ionizing radiation sources; maintaining the security of, and access to, ionizing radiation sources; and recognizing and responding appropriately to incidents involving ionizing radiation sources to prevent the spread of contamination;

- (6) Ensuring through coordination with the Radiation Facility Owner that all individuals who have unescorted, unsupervised access to the source, or can exercise material control of the source, are appropriately trained for such access;
- (7) Ensuring that procedures and engineering controls are used to keep occupational doses and doses to members of the public ALARA;
- (8) Identifying to their Group Leader and Gaithersburg RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications; and
- (9) Coordinating with the HP Group any transfers of custodianship, changes in utilization, shipments of sources to off-site entities, or disposal of waste;
- (10) Maintaining source inventory records of utilization, decay-corrected activity, transfer, and disposal;
- (11) Performing physical inventory verifications and reconciling documentary records as necessary;
- (12) Notifying the NIST Gaithersburg RSO of any known occupational radiation exposure due to work at facilities other than NIST;
- (13) Ensuring that ionizing radiation sources on their inventory are used safely and in accordance with regulatory and NIST radiation safety program requirements;
- (14) Providing appropriate oversight of their Source Users; and
- (15) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

u. Reactor Operators are responsible for:

- (1) The safe operation of the NBSR within the NBSR Technical Specifications and the TR-5 License.
- (2) Ensuring that reactor operations are conducted in accordance with the ANS Radiation Protection at Research Reactors (ANS 15.11) standard and the NCNR ALARA program.

v. NCNR Users are responsible for:

- (1) Identifying to the Reactor Facility Group Leader any issues that have, or may have, radiological safety concerns or regulatory compliance implications;
- (2) Ensuring that ionizing radiation sources (e.g., activated beam samples and calibration sources) in their labs or areas are used, handled, and stored safely and in accordance with regulatory and NIST radiation safety program requirements;

(3) Ensuring that ionizing radiation sources, including neutron beam and in-core irradiated samples, are properly transferred into and out of the NCNR;

(4) Completing appropriate training, including all training required by the TR-5 and other applicable licenses, if any, and by the NIST radiation safety program, including training on the safe use of ionizing radiation sources; maintaining the security of, and access to, ionizing radiation sources; and recognizing and responding appropriately to incidents involving ionizing radiation sources to prevent the spread of contamination; and

(5) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

w. Source Users are responsible for:

(1) Using, handling, or manipulating only sources for which they have been approved by the RSO or designee, the Source Custodian for those sources, and authorized by Management;

(2) Using ionizing radiation sources in a manner that complies with the terms and conditions specified in the NIST-364 form and associated documents, and in any applicable NIST-365 forms, specific to the source(s) being used, including use protocols and hazard mitigation and emergency response plans;

(3) When appropriate, initiating requests using the NIST-365 form for changes in the utilization of radioactive material, or in Source User(s) or use and storage locations, in coordination with the pertinent Source Custodian;

(4) Completing all training required by the NIST radiation safety program, including training on the safe use of ionizing radiation sources; maintaining the security of, and access to, ionizing radiation sources; and recognizing and responding appropriately to incidents involving ionizing radiation sources to prevent the spread of contamination;

(5) Ensuring that engineering and administrative controls are used to keep occupational doses and doses to members of the public ALARA;

(6) Identifying to their respective Source Custodian any issues that have, or may have, radiological safety concerns or regulatory compliance implications;

(7) Notifying the RSO of any known occupational radiation exposures due to work at facilities other than NIST; and

(8) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

x. Authorized Users are responsible for:

(1) Using, handling, or manipulating only those sources for which they have been approved by the NIST Boulder RSO, the IRSC, and the NRC, if necessary, and authorized by Management;

- (2) Completing, as part of requests made using NIST/BL-100 and NIST/BL-101 forms, the appropriate hazard assessments and establishing the hazard mitigation and emergency response plans, if applicable, for their ionizing radiation sources through coordination with the Boulder RSO;
- (3) Using ionizing radiation sources in a manner that complies with the terms and conditions specified in the NIST/BL-100 form and associated documents, and in any applicable NIST/BL-101 forms, specific to the sources being used, including use protocols and hazard mitigation and emergency response plans;
- (4) When appropriate, initiating requests using the NIST/BL-101 form for changes in the utilization of radioactive material, or in Authorized User(s), Supervised User(s), or use and storage locations;
- (5) Completing all training required by the NIST radiation safety program, including training on the safe use of ionizing radiation sources; maintaining the security of, and access to, ionizing radiation sources; and recognizing and responding appropriately to incidents involving ionizing radiation sources to prevent the spread of contamination;
- (6) Ensuring that engineering and administrative controls are used to keep occupational doses and doses to members of the public ALARA;
- (7) Identifying to the Boulder RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;
- (8) Providing direct oversight of their Supervised Users;
- (9) Maintaining source inventory records of utilization, decay-corrected activity, transfer, and disposal; and
- (10) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

y. Supervised Users are responsible for:

- (1) Using, handling, or manipulating only those sources for which they have been approved by the NIST Boulder RSO and the IRSC, and authorized by Management;
- (2) Using ionizing radiation sources in a manner that complies with the terms and conditions specified in the NIST/BL-100 form and associated documents, and in any applicable NIST/BL-101 forms, specific to the source(s) being used, including use protocols and hazard mitigation and emergency response plans;
- (3) Completing all training required by the NIST radiation safety program, including training on the safe use of ionizing radiation sources; maintaining the security of, and access to, ionizing

radiation sources; and recognizing and responding appropriately to incidents involving ionizing radiation sources to prevent the spread of contamination;

(4) Ensuring that engineering and administrative controls are used to keep occupational doses and doses to members of the public ALARA;

(5) Identifying to their respective Authorized User any issues that have, or may have, radiological safety concerns or regulatory compliance implications; and

(6) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

z. Radioactive Material Package Receivers are responsible for:

(1) Completing all training required by the NIST radiation safety program;

(2) Ensuring that radioactive packages remain secured from unauthorized access or removal until delivered to a member of the HP Group or the Boulder RSO, as applicable;

(3) Immediately notifying a member of the HP Group or Boulder RSO, as applicable, if there is any evidence of type of damage or degradation of package integrity such as packages that are crushed, wet, or otherwise damaged; and

(4) Immediately notifying a member of the HP Group or the Boulder RSO, as applicable, if a radioactive package becomes unaccounted for.

aa. Ionizing-Radiation-Producing Device Users are responsible for:

(1) Ensuring that all proposed experiments or modifications of ionizing-radiation-producing devices or Radiation Facilities have been approved by the appropriate RSO and authorized by Management prior to initiation of work or implementation of changes;

(2) Complying with the terms and conditions specified in the approved protocols and operating procedures for the specific ionizing-radiation-producing device, including any hazard mitigation and emergency response plans;

(3) Completing all training required by the NIST radiation safety program, including training on the safe use of the specific ionizing-radiation-producing device, and recognizing and responding appropriately to incidents involving the ionizing-radiation-producing device;

(4) Ensuring that the ionizing-radiation-producing device is used in a Radiation Facility approved by the appropriate RSO and authorized by Management, and that all safety and control equipment is functional;

(5) Ensuring that engineering and administrative controls are used to keep occupational doses and doses to members of the public ALARA;

- (6) Identifying to their supervisor and the appropriate RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications;
- (7) Notifying the appropriate RSO of any known occupational radiation exposure due to work at facilities other than NIST; and
- (8) Complying with the requirements of NIST Laboratory Safety Manual, Chapter 8, Radiation Safety.

bb. NIST Employees and non-NIST Personnel are responsible for:

- (1) Completing required training commensurate with their duties, and completing refresher training in accordance with license and regulatory requirements or as research protocols, procedures, or duties change; and
- (2) Identifying to their supervisor and the appropriate RSO any issues that have, or may have, radiological safety concerns or regulatory compliance implications.

cc. Individuals Interacting with the NRC are responsible for:

- (1) Providing information to the NRC that is complete and accurate in all material respects.

12.03.10

ENFORCEMENT

- a. NIST is subject to inspections by Federal and State entities. Inspectors for these entities have the right and authority to evaluate the regulatory compliance aspects of all individuals and facility operations under the purview of the NRC licenses held by NIST and, in Boulder, of the Colorado State Board of Health, Radiation Control.
- b. Individuals whose assigned duties involve the use of or exposure to ionizing radiation sources at Gaithersburg or Boulder or the Reactor Facility at Gaithersburg are subject to monitoring, surveillance, and audits by the NRC, the IRSC, the Gaithersburg RSO and HP Group, and the Boulder RSO.
- c. Findings resulting from inspections, monitoring, surveillance, and audits noted in 12.03.10a and 12.03.10b may result in suspension or termination of use of ionizing radiation sources at NIST and by specific individuals, and of access to Radiation Facilities and the Reactor Facility. Failure to comply with established policies and procedures may result in disciplinary action. Violations of license requirements, including failure to provide information to the NRC that is complete and accurate in all material respects, have the potential for civil and criminal penalties.

12.03.11

CONTENT OWNER

Chief Safety Officer (CSO)

12.03.12**EFFECTIVE DATE**

August 17, 2010.

12.03.13**REFERENCES**

- a. NRC License Numbers SNM-362, 19-23545-01E, 05-03166-05, and TR-5 (including Technical Specifications).
- b. Applicable Parts of Title 10, Code of Federal Regulations: Nuclear Regulatory Commission.
- c. Applicable Parts of Title 29, Code of Federal Regulations: Labor.
- d. Applicable Parts of Title 40, Code of Federal Regulations: Protection of the Environment.
- e. Applicable Parts of Title 49, Code of Federal Regulations: Transportation.

ANIMAL CARE AND USE

Sections

14.02.01 Purpose

14.02.02 Scope

14.02.03 Policy

14.02.04 References

14.02.05 Definitions

14.02.06 Responsibilities

14.02.07 Delegations of Authority

Appendix A - Utilization and Care of Vertebrate Animals Used in Testing, Research and Training

Appendix B - Health Research Extension Act of 1985: "Animals in Research"

14.02.01

PURPOSE

This subchapter establishes responsibility for humane care and use of animals within the NIST program.

14.02.02

SCOPE

This policy is applicable to all NIST-conducted or supported activities involving animals, whether the activities are performed at NIST, an awardee institution, or any other institution, and conducted in the United States, the Commonwealth of Puerto Rico, or any territory or possession of the United States. The requirements of this policy are effective for applications and proposals for NIST research involving animals that are submitted for NIST consideration, and for all NIST-conducted or -supported research involving animals. Institutions in foreign countries receiving NIST support for activities involving animals shall comply with this policy, or provide evidence to NIST that acceptable standards for the humane care and use of the animals in the NIST-conducted or supported activities will be met. No NIST support for an activity involving animals will be provided to an individual unless that individual is affiliated with or sponsored by an institution which can and does assume responsibility for compliance with this subchapter, unless the individual makes other arrangements with the NIST. This policy does not affect applicable state or local laws or regulations which impose more stringent standards for the care and use of laboratory animals. All NIST components, contractors, or institutions with which NIST has collaborative or cooperative agreements are required to comply, as applicable, with all federal statutes and regulations relating to animals. This policy is also

applicable to the transportation of experimental animals on NIST property, between buildings or facilities, to or from commercial carriers, or in any other manner.

14.02.03

POLICY

The NIST policy is that each investigator or person involved in the care or use of animals adhere to the Principles, the Guide, and applicable humane and ethical policies as established or referenced herein, including the Animal Welfare Act, the Health Research Extension Act of 1985, and the Endangered Species Act of 1973. Adequate veterinary care shall conform to the standards set forth in the Guide and in Adequate Veterinary Care. The NIST-Animal Care and Use Committee (NIST-ACUC) will suspend any activity involving animals that has been previously approved if it is determined that the activity is not being conducted in accordance with the previously approved animal study proposal or provisions cited in this subchapter.

14.02.04

REFERENCES

a. Laws –

- (1) Animal Welfare Act (7 U.S.C. 2131 et seq).
- (2) The Endangered Species Act of 1973 (16 U.S.C. 1531 et seq).
- (3) Health Research Extension Act of 1985 (Pub.L. 99-158, November 20, 1985).

b. Regulations –

- (1) Good Laboratory Practice for Nonclinical Laboratory Studies (FDA Regulations Title 21, CFR, Part 58, 1976).
- (2) Procurements Involving the Use of Laboratory Animals (Federal Acquisition Regulations Supplement, Clause 52.235-7003).

c. Policies –

- (1) Guide for the Care and Use of Laboratory Animals (DHHS Publication No. NIH 85-23).
- (2) PHS Policy on Humane Care and Use of Laboratory Animals, Sept. 1986.
- (3) Report of the AVMA Panel on Euthanasia, JAVMA 183 (3): 252-268, February 1, 1986.
- (4) Biosafety in Microbiological and Biomedical Laboratories, March 1984. DHHS Publication No. (CDC) 84-8395.

(5) The National Institutes of Health Radiation Safety Guide (DHHS Publication No. (NIH) 79-18).

(6) Institutional Administrator's Manual for Laboratory Animal Care and Use (DHHS Publication No. (NIH) 88-2959).

d. Guidelines -

Report of the American College of Laboratory Animal Medicine (ACLAM) on Adequate Veterinary Care, October 1986.

14.02.05

DEFINITIONS

a. Accreditation - Recognition by the American Association for Accreditation of Laboratory Animal Care or other NIST-approved accrediting body that the animal facilities and management practices of a research institution are in accordance with the Public Health Service/National Institutes of Health Guide for Care and Use of Animals (Guide).

b. Adequate Veterinary Care - Care conforming to the standards set forth in the Guide and in Adequate Veterinary Care by the American College of Laboratory Animal Medicine.

c. Animal - Any live, vertebrate animal used or intended for use in research, experimentation, testing, training, or related purposes. (The acquisition and transportation of certain invertebrates and of parts of certain vertebrates are also subject to federal regulation.)

d. Animal Facility - Any and all buildings, rooms, areas, enclosures, or vehicles, including satellite facilities, used for animal confinement, transport, maintenance, breeding, or experiments inclusive of surgical manipulation. A satellite facility is any containment outside of a core facility or centrally designated or managed area in which animals are housed for more than 24 hours.

e. Form NIST-1258, Contractor/Grantee Animal Study Proposal, and Form NIST-1259, Intramural Animal Study Proposal - supplied by the NIST Animal Care and Use Committee (NIST-ACUC), completed by an intramural or extramural Principal Investigator and submitted for approval to the Chair of the NIST-ACUC prior to the ordering of animals or initiation of study. (Copies of these forms are available from the NIST-ACUC).

f. Guide - The Public Health Service (PHS)/National Institutes of Health (NIH) Guide for the Care and Use of Laboratory Animals, which serves as the standard by which animal care and use programs are developed and assessed. The Guide is available from the NIST-ACUC or the Office of Animal Care and Use (OACU), O.D., NIH, Building 12A, Room 4003, Bethesda, MD 20892, (301) 496-5424.

g. NIST Animal Care and Use Committee (NIST-ACUC) - The NIST Animal Care and Use Committee which is appointed by the NIST Director and composed of a Chair and members as defined in Subchapter 3.01, Appendix A.

h. NIST Veterinary Advisor - A Doctor of Veterinary Medicine, with training or experience in laboratory animal science and medicine, who is a member of the NIST-ACUC and provides advice for activities involving animals at NIST.

i. Principles - U.S. Government Principles for the Utilization and Care of Vertebrate Animals Used in Testing, Research and Training (See Appendix A).

j. Principal Investigator - The scientist responsible for conducting an animal study in compliance with this subchapter and the Guide, and who certifies acceptance of this responsibility by signing Form NIST-1259. "Intramural" Principal Investigators are NIST employees who are responsible for such research performed in NIST facilities. "Extramural" Principal Investigators are employees of institutions who are responsible for such research in non-NIST facilities as a result of a grant or contract with NIST.

k. Proposal - A research or contract plan containing a description of the research, the necessity for the study, a detailed work plan, and budget.

l. Technical Officer - The NIST scientist or engineer who is responsible for and provides technical oversight for a research project carried out under a NIST grant or contract. In the case of NIST grants, this individual is commonly known as the "Scientific Officer." In the case of NIST contracts, this individual is commonly known as the "Contracting Officer's Technical Representative (COTR)."

14.02.06

RESPONSIBILITIES

a. The NIST Director - Responsible for ensuring compliance with this subchapter by all NIST employees, contractors, grantees, and others that are funded by NIST or use NIST facilities; for implementing and administering this subchapter; and for taking appropriate action regarding recommendations from the NIST-ACUC.

b. Intramural Principal Investigators - The NIST Principal Investigator shall:

(1) Secure the division chief's approval of the scientific merit and funding for any research involving animals.

(2) Sign and submit a completed Form NIST-1259 along with a copy of the division chief-approved research proposal, to the OU and the ACUC for review before requesting animals or initiating animal studies.

(3) Attend the course, Using Animals in Research: Guidelines for Investigators or participate in a comparable training experience approved by the ACUC, prior to approval of Form NIST-1259. (This policy may be waived by the ACUC until the next offering of

the course.)

(4) Ensure all personnel working with animals on the project receive training in the appropriate techniques for the species of animals that they use.

(5) Comply with this subchapter and the Guide.

(6) Ensure that the NIST-ACUC is informed in writing of proposed significant deviations from procedures described on Form NIST-1259.

c. Extramural Principal Investigator - The Extramural Principal Investigator shall submit to the NIST Technical Officer:

(1) A grant or contract Proposal.

(2) A completed Form NIST-1258 with signed approval by the Institutional ACUC.

(3) Copies of other governmental approvals for their animal care and use procedures and showing the current status of their assurance by PHS/NIH, and copies of animal care facility accreditation.

(4) Certification that the Principal Investigator and other personnel involved in the care and use of the animals are trained as required by this subchapter and the Guide.

During the course of the research, the Extramural Principal Investigator must inform the NIST Technical Officer in writing of any proposed deviation from procedures involving animals described on Form NIST-1258, any change in personnel and their training, any change in the status of their PHS/NIH assurance or other governmental inspecting bodies; and the results of any inspections of their animal care facilities that take place during the course of the contract or grant.

d. NIST Technical Officer - The NIST Technical Officer shall:

(1) Secure scientific and management approval of the extramural research Proposal via normal NIST procedures.

(2) Forward the approved Proposal to the NIST-ACUC for its review and approval.

(3) Inform the NIST-ACUC of any information from the Contractor/Grantee that deviates from the animal-related information supplied in the Proposal or on Form NIST-1258, throughout the duration of the contract or grant.

e. NIST Veterinary Advisor - The NIST Veterinary Advisor shall:

(1) Advise on implementation of the NIST Animal Care and Use Program.

(2) Help the NIST-ACUC evaluate compliance with this subchapter and the Guide in the animal facility(ies).

(3) Advise the Principal Investigator or Technical Officer, the NIST-ACUC, and the NIST Director on activities involving animals at NIST, to ensure compliance with this subchapter and the Guide.

14.02.07

DELEGATIONS OF AUTHORITY

The NIST Director delegates authority to:

- a. The NIST Animal Care and Use Committee (NIST-ACUC) to monitor implementation;
- b. The NIST OU Directors to implement and administer this policy on a day-to-day basis for each organizational unit that uses animals in research, and for taking appropriate action regarding recommendations from the NIST-ACUC;
- c. The Principal Investigator to ensure compliance in every day operations, such as the experimental setting and procedures, veterinary care, husbandry, and provision of supplies and equipment; and
- d. The NIST Veterinary Advisor to evaluate veterinary compliance with this NIST subchapter and the Guide.

APPENDIX A

UTILIZATION AND CARE OF VERTEBRATE ANIMALS USED IN TESTING, RESEARCH AND TRAINING*

The development of knowledge necessary for the improvement of the health and well-being of humans as well as other animals requires in vivo experimentation with a wide variety of animal species. Whenever U.S. government agencies develop requirements for testing, research, or training procedures involving the use of vertebrate animals, the following principles shall be considered; and whenever these agencies actually perform or sponsor such procedures, the responsible institutional official shall ensure that these principles are adhered to:

1. The transportation, care, and use of animals should be in accordance with the Animal Welfare Act (7 U.S.C. 2131 et. seq.) and other applicable federal laws, guidelines, and policies.
2. Procedures involving animals should be designed and performed with due consideration of their relevance to human or animal health, the advancement of knowledge, or the good of society.
3. The animals selected for a procedure should be of an appropriate species and quality and the minimum number required to obtain valid results. Methods such as mathematical models, computer simulation, and in vitro biological systems should be considered.
4. Proper use of animals, including the avoidance or minimization of discomfort, distress, and pain when consistent with sound scientific practices, is imperative. Unless the contrary is established, investigators should consider that procedures that cause pain or distress in human beings may cause pain or distress in other animals.
5. Procedures with animals that may cause more than momentary or slight pain or distress should be performed with appropriate sedation, analgesia, or anesthesia. Surgical or other painful procedures should not be performed on unanesthetized animals paralyzed by chemical agents.
6. Animals that would otherwise suffer severe or chronic pain or distress that cannot be relieved should be painlessly killed at the end of the procedure or, if appropriate, during the procedure.
7. The living conditions of animals should be appropriate for their species and contribute to their health and comfort. Normally, the housing, feeding, and care of all animals used for biomedical purposes must be directed by a veterinarian or other scientist trained and experienced in the proper care, handling, and use of the species being maintained or studied. In any case, veterinary care shall be provided as indicated.

8. Investigators and other personnel shall be appropriately qualified and experienced for conducting procedures on living animals. Adequate arrangements shall be made for their in-service training, including the proper and humane care and use of laboratory animals.

9. Where exceptions are required in relation to the provisions of these principles, the decisions should not rest with the investigators directly concerned but should be made, with due regard to Principle 2, by an appropriate review group such as an institutional animal research committee. Such exceptions should not be made solely for the purposes of teaching or demonstration.

*Published in the Federal Register, May 20, 1985, Vol. 50, No. 97, pp. 20864-20865, by the Office of Science and Technology Policy.

APPENDIX B
HEALTH RESEARCH EXTENSION ACT OF 1985: "ANIMALS IN
RESEARCH"1

Sec. 495.

(a) The Secretary, acting through the Director of NIH, shall establish guidelines for the following:

(1) The proper care of animals to be used in biomedical and behavioral research.

(2) The proper treatment of animals while being used in such research. Guidelines under this paragraph shall require--

(A) the appropriate use of tranquilizers, analgesics, anesthetics, paralytics, and euthanasia for animals in such research; and

(B) appropriate pre-surgical and post-surgical veterinary medical and nursing care for animals in such research.

Such guidelines shall not be construed to prescribe methods of research.

(3) The organization and operation of animal care committees in accordance with subsection (b).

(b) (1) Guidelines of the Secretary under subsection (a)(3) shall require animal care committees at each entity which conducts biomedical and behavioral research with funds provided under this Act (including the National Institutes of Health and the national research institutes) to assure compliance with the guidelines established under subsection (a).

(2) Each animal care committee shall be appointed by the chief executive officer of the entity for which the committee is established, shall be composed of not fewer than three members, and shall include at least one individual who has no association with such entity and at least one doctor of veterinary medicine.

(3) Each animal care committee of a research entity shall--

(A) review the care and treatment of animals in all animal study areas and facilities of the research entity at least semiannually to evaluate compliance with applicable guidelines established under subsection (a) for appropriate animal care and treatment;

(B) keep appropriate records of reviews conducted under subparagraph (A); and

(C) for each review conducted under subparagraph (A), file with the Director of NIH at least annually (i) a certification that the review has been conducted, and (ii) reports of any violations of guidelines established under subsection (a) or assurances required under

paragraph (1) which were observed in such review and which have continued after notice by the committee to the research entity involved of the violation. Reports filed under subparagraph (C) shall include any minority views filed by members of the committee.

(c) The Director of NIH shall require each applicant for a grant, contract, or cooperative agreement involving research on animals which is administered by the National Institutes of Health or any national research institute to include in its application or contract proposal, submitted after the expiration of the twelve-month period beginning on the date of enactment this section--

(1) Assurances satisfactory to the Director of NIH that--

(A) the applicant meets the requirements of the guidelines established under paragraphs (1) and (2) of subsection (a) and has an animal care committee which meets the requirements of subsection (b); and

(B) scientists, animal technicians, and other personnel involved with animal care, treatment, and use by the applicant have available to them instruction or training in the humane practice of animal maintenance and experimentation, and the concept, availability, and use of research or testing methods that limit the use of animals or limit animal distress; and

(2) a statement of the reasons for the use of animals in the research to be conducted with funds provided under such grant or contract. Notwithstanding subsection (a)(2) of Section 553 of Title 5, United States Code, regulations under this subsection shall be promulgated in accordance with the notice and comment requirements of such section.

(d) If the Director of NIH determines that--

(1) the conditions of animal care, treatment, or use in an entity which is receiving a grant, contract, or cooperative agreement involving research on animals under this title do not meet applicable guidelines established under subsection (a);

(2) the entity has been notified by the Director of NIH of such determination and has been given a reasonable opportunity to take corrective action; and

(3) no action has been taken by the entity to correct such conditions; the Director of NIH shall suspend or revoke such grant or contract under such conditions as the Director determines appropriate.

(e) No guideline or regulation promulgated under subsection (a) or (c) may require a research entity to disclose publicly trade secrets or commercial or financial information which is privileged or confidential.

1/ Public Law 99-158, November 20, 1985.

Chapter 14 Special Program Activities

Subchapter 14.05 Standard Reference Data Program

Sections

14.05.01 Purpose

14.05.02 Scope

14.05.03 Objective

14.05.04 Responsibilities

14.05.05 Special Services by Data Centers

14.05.06 Cost of Services

14.05.07 Calculation of Charges

14.05.08 Exemptions from Charges

14.05.09 Collection of Charges

14.05.10 Use of Funds Collected

14.05.11 Reporting Procedure

14.05.12 Other SRDP Functions

14.05.13 Outside Data Centers

14.05.14 Other SRDP-Supported Projects

14.05.15 Review of New Substantial Standard Reference Data Projects

14.05.01

PURPOSE

This subchapter primarily contains guidelines for special services performed by the Standard Reference Data Program (SRDP) data centers within NIST. It also contains information concerning outside data centers under contract to SRDP (1) funded solely by NIST and (2) funded jointly by NIST and other agencies (see Section 14.05.13).

14.05.02

SCOPE

This subchapter applies to NIST-Gaithersburg and NIST-Boulder.

14.05.03

OBJECTIVE

The primary objective of the Standard Reference Data Program is to make critically evaluated reference data readily available to scientists, engineers, and the general public, through published tables, computer diskettes, and other dissemination mechanisms that reach a broad section of the technical community. Except in special circumstances, each project supported by SRDP will have as its main goal the preparation of data for broad distribution in this manner. The normal channels of distribution are the Journal of Physical and Chemical Reference Data, appropriate NIST publication series, private publishers under contract to SRDP, PC diskettes, and other modes developed by SRDP.

14.05.04

RESPONSIBILITIES

- a. The leader of each data center, in consultation with the Chief, Standard Reference Data Program will establish the schedule of charges for that data center relating to special services performed by the data center. SRDP should be consulted when any change in this schedule is proposed.
- b. Data center leaders have the authority to waive charges on the grounds listed in Section 14.05.08. Charges may still be made, at the discretion of the data center leader, even if one or more of the conditions for waiver apply.
- c. Waiver of charges greater than \$500 must be approved by the Chief, Standard Reference Data Program.

14.05.05

SPECIAL SERVICES BY DATA CENTERS

- a. In order to prepare data for critical evaluation and subsequent publication, several preliminary steps are required, such as retrieval of papers from the literature, indexing, and extraction and organization of data. In this way each continuing data center develops files that provide comprehensive coverage of its field of interest. These files, together with the expertise of the staff, represent a resource that has other potential uses. For example, they can serve as a base for answering inquiries for specific data, for preparing selective bibliographies on request, and for selective dissemination of information or current awareness services.
- b. Data centers are encouraged to respond to such requests and to provide other useful services that do not interfere significantly with their progress toward the primary goal of preparing evaluated data for publication.

14.05.06

COST OF SERVICES

The cost of these special services by data centers should be charged to the individual or organization for which they are provided, unless there are circumstances which justify waiving the charges. In determining the charges, only the incremental costs incurred in providing the service should be considered, since the cost of developing the database is properly charged to the project supporting the data center. These incremental costs include:

- (1) Labor of data center personnel (including overhead) required to perform the service.
- (2) Cost of computer related activity, including literature searches.
- (3) Cost of any additions to the database made specifically for the purpose of providing the service.
- (4) Any other costs that would not be incurred in the absence of the service in question.

14.05.07

CALCULATION OF CHARGES

- a. Labor - To simplify bookkeeping, a standardized charge of \$25/hour for clerical labor and \$60/hour for professional labor will be made.
- b. Computer - Either actual cost for each search, calculation, or any other computer activity, or a standardized schedule of charges for specified types of activity. In the latter case, the schedule should reflect the average cost of searches and must be approved by SRDP.
- c. Current Awareness Services - Prices should reflect the cost of preparation, printing, and mailing.
- d. Other - Actual cost.

14.05.08

EXEMPTIONS FROM CHARGES

- a. Charges for special services may be waived on any of the following grounds:
 - (1) The time required is four hours or less and the total of other costs is less than \$500.
 - (2) The service is performed for a member of the NIST staff.
 - (3) The requester has made (or is expected to make) contributions to the Standard Reference Data Program through supplying data or other information, carrying out evaluations, reviewing manuscripts, advising on program priorities, etc.

(4) The service is provided for another data center on an exchange basis.

(5) The request is concerned with the evaluation procedures of the data center and is thus materially related to the credibility of the data center's output.

(6) The request comes from another government agency or from Congress and is of sufficient importance to justify waiving of charges.

14.05.09

COLLECTION OF CHARGES

When it is determined that a charge should be made for a particular service, the data center should inform the requester of the estimated amount and obtain concurrence, preferably in writing, before proceeding with the work. After the service is completed, a form (available in SRDP) should be submitted to SRDP with full information required for billing. SRDP will follow the established mechanism for billing and collection, through the Office of the Comptroller.

14.05.10

USE OF FUNDS COLLECTED

SRDP funding of data centers is predicated on the delivery of a tangible product to SRDP, while the provision of other services represents a diversion of resources from this primary goal. To avoid interference with the commitments of the data center to SRDP, all funds collected from the services of a data center will be returned to that data center.

14.05.11

REPORTING PROCEDURE

Data centers will keep records of services provided, including a notation of the grounds for waiving charges when this is done. Reports should be submitted to SRDP if charges are collected. A simplified reporting form used by the data center is acceptable if it includes the required information.

14.05.12

OTHER SRDP FUNCTIONS

In addition to the responsibilities detailed above, SRDP will refer all inquiries and requests received to the appropriate data center. If no data center exists in the technical area covered by the request, SRDP will attempt to refer the requester to an appropriate expert at NIST or elsewhere. If the request can be satisfied easily by the SRDP staff (specifically, with the expenditure of no more than one hour of staff time), SRDP may respond directly. In general, services requiring greater staff time will not be performed by SRDP for individual requesters. However, such services as are provided by SRDP will be subject to the same provisions regarding charges and waiver requirements that apply to the data center.

14.05.13

OUTSIDE DATA CENTERS

a. The guidelines in this subchapter are primarily for SRDP data centers within NIST. They also apply, with necessary modifications, to outside data centers under contract to SRDP. In the case of outside data centers, the following situations must be considered:

(1) Joint funding by SRDP and another agency for a single class of output - A procedure consistent with the policies of both agencies will be established by negotiation. User charges that are collected will be apportioned between agencies according to the funding ratio. The SRDP portion will be retained by the data center in accordance with the principle outlined in Section 14.05.10.

(2) Joint funding of a data center in which a class of outputs can be identified exclusively with the SRDP portion of the funding - Procedure will be established by negotiation. User charges collected by the data center that are identifiable with the scope of SRDP support will be reported to SRDP. In accordance with the principle outlined in 14.05.10, these funds will be retained by the center.

(3) Sole funding by SRDP - Procedures consistent with the guidelines in this subchapter will be negotiated with the data center. Charges may be collected and retained by the data center if this is more efficient, but reports will be submitted to SRDP as described in Section 14.05.11.

14.05.14

OTHER SRDP-SUPPORTED PROJECTS

SRDP supports a number of projects that cannot be characterized as data centers because of their narrow technical scope and limited time span. Such projects do not lead to comprehensive files and other facilities upon which services of the type described above can be based. When a NIST staff member engaged in such a project responds to a request for technical information, this activity is considered to fall under the general provisions for NIST Consulting and Advisory Services. Thus no specific reporting or accounting will be required by SRDP. Similar projects conducted by SRDP contractors outside NIST will not be subject to user charge requirements.

14.05.15

REVIEW OF NEW SUBSTANTIAL STANDARD REFERENCE DATA PROJECTS

a. Background - To carry out an effective information dissemination program, knowledge of the marketplace in which the information dissemination product is to be placed is useful. To design the best possible product and to minimize the instances of duplication, before a substantial project is undertaken NIST should consider whether or not particular information dissemination needs have been met by others. Any consideration should include communication and consultation with the users and providers of particular information dissemination products. Adequate notice of information dissemination plans and an opportunity to comment on those plans should be

part of the consideration. In certain circumstances the responsibility to disseminate information may be independent of the availability of similar information dissemination products, even where another public or private entity has offered a similar information dissemination product. In those instances, NIST may conclude that despite the availability of similar projects, there is nonetheless a responsibility to disseminate NIST's own product.

b. Policy - As part of its responsibilities under 15 U.S.C. 290 to collect, evaluate, and publish high-quality Standard Reference Data (SRD), NIST creates SRD databases. NIST acknowledges the desirability to minimize duplication, overlap, and competition with similar private sector databases. Duplication, overlap, and competition can be minimized by giving consideration to comments from interested parties and peers and by giving consideration to the merits and drawbacks of creating or modifying SRD databases. It is therefore NIST policy that substantial SRD database projects which may compete with private sector databases shall be created or significantly added to only after the proposed database project has been evaluated in accordance with the procedures listed below. In addition, the NIST Board of Assessment will peer review NIST Standard Reference Data activities on a regular basis.

c. Procedures - Before creation or modification of a substantial SRD database, the chief of the division proposing the new or revised database should:

(1) Publish in the Federal Register or the Commerce Business Daily or in a similar publication, notice of the proposed action and provide at least 15 days for comments from interested parties. The notice may invite interested parties to attend meetings or workshops;

(2) Request that the NIST Standard Reference Data Program publish notice on its web page of the proposed action and provide an opportunity to comment;

(3) Consider the need in the scientific community for the proposed action;

(4) Consider the impact of the proposed action on similar existing private-sector databases; and

(5) Make a written determination as to the need for the proposed action, including a finding as to whether or not the mission of NIST or the SRDP outweighs any concerns raised.

NIST DIRECTIVES INVENTORY

Title	Type	Number	OU
Forms Management	Procedure	PR 1000.05	M&O
Administrative Committees	Order	O 1005.00	M&O
Organizational Changes	Order	O 1007.00	M&O
Contacts with Congress and others	Order	O 1030.00	CLAO
Procedures for Transmittal of Advisory Committee Reports to Congress	Procedure	PR 1030.01	CLAO
Clearance for Reports to Congress - Authorization	Procedure	PR 1030.02	CLAO
Drafting and Clearance Procedures for Reports to Congress - Appropriations	Procedure	PR 1031.01	OFRM
Public Communications	Order	O 1074.00	PAO
Conferences and Meetings	Order	O 1075.00	PAO
Directives Management System	Policy	P 1100.00	M&O
Directives Management System	Order	O 1110.00	M&O
Equal Employment Opportunity (EEO) and Diversity	Policy	P 1200.00	CRDO
Visiting Researcher and Associate Policy	Policy	P 1400.00	COS
Foreign Visitors	Procedure	PR 1400.01	IAAO
Domestic Associates Program	Order	O 1401.00	TPO
Use of the Emeritus Title	Notice	N 1401.01	TPO
Domestic Associates Program Procedures	Procedure	PR 1401.01	TPO
Foreign Guest Researcher Program	Order	O 1402.00	IAAO
Foreign Guest Researcher Program Procedures	Procedure	PR 1402.01	IAAO
New Category of Foreign Guest Researcher	Notice	N 1402.01	IAAO
Letters to Support Petitions for United States Legal Permanent Residency	Order	O 1403.00	IAAO
Research Library, Publishing, and Museum Services	Policy	P 1500.00	ISO
Research Library Services	Order	O 1501.00	ISO
Procedures for Borrowing Information Resources and E-Devices from the NIST Research Library	Procedure	PR 1501.01	ISO
Publishing Services - NIST Technical Series Publications and the Journal of Research of the NIST	Order	O 1502.00	ISO
Records Management	Policy	P 1600.00	M&O
Web Content	Policy	P 1700.00	PAO
Web Content Requirements	Order	O 1701.00	PAO
Review of Fundamental Research Communications	Policy	P 1800.00	ADLP
Review of Fundamental Research Communications	Order	O 1801.00	ADLP
Review of Scholarly and Technical Manuscripts Intended for Publication	Suborder	S 1801.01	ADLP
Review of Data Intended for Publication	Suborder	S 1801.02	ADLP

NIST DIRECTIVES INVENTORY

Title	Type	Number	OU
Review of Software Intended for Publication	Suborder	S 1801.03	ADLP
Review of Scholarly and Technical Videos Intended for Publication	Suborder	S 1801.04	ADLP
Facilities and Site Management	Policy	P 2100.00	OFPM
Laboratory and Work Space Decommissioning	Procedure	PR 2100.01	OFPM
Personal Property Management Program	Order	O 2102.00	OFPM
Facilities and Site Management	Order	O 2103.00	OFPM
Acquisition and Disposal of Real Property	Suborder	S 2103.05	OFPM
Leasing of Real Property	Suborder	S 2103.06	OFPM
Mail Management	Procedure	PR 2103.05	OFPM
Site Access during Site Closure and Delayed Openings	Order	O 2105.00	OFPM
Transportation Program	Order	O 2106.00	OFPM
Traffic and Parking	Procedure	PR 2106.01	ESO
Transit Subsidy Program	Procedure	PR 2106.02	OFPM
Bicycle Parking Notice	Notice	N 2106.01	ESO
Energy and Sustainability Management Program	Order	O 2107.00	OFPM
Export Control Management Program	Order	O 2108.00	OFPM
Space Management and Utilization	Order	O 2109.00	OFPM
Space Management and Utilization	Procedure	PR 2109.01	OFPM
Emergency Management	Policy	P 2200.00	ESO
Emergency Management Program	Order	O 2201.00	ESO
Energy Contingencies	Procedure	PR 2201.03	OFPM
Smoking Policy	Policy	P 2300.00	OFPM
Security	Policy	P 2400.00	ESO
Facility Access Cards and Electronic Access Control	Procedure	PR 2401.01	ESO
Human Resources Management	Policy	P 3100.00	OHRM
Telework Program	Order	O 3102.00	OHRM
NIST NRC Postdoctoral Research Associateship Program	Order	O 3105.00	IAAO
NIST NRC Postdoctoral Research Associate Program	Procedure	PR 3105.01	IAAO
Employment of Non-U.S. Citizens	Order	O 3112.00	OHRM
Employment of Non-U.S. Citizens	Procedure	PR 3112.01	OHRM
Merit Assignment Plan	Order	O 3113.00	OHRM
Associate Entrance on Duty and Separation Clearance	Order	O 3114.00	OHRM

NIST DIRECTIVES INVENTORY

Title	Type	Number	OU
Separation Clearance	Order	O 3115.00	OHRM
Disciplinary/Adverse Actions	Order	O 3120.00	OHRM
Incentive Awards	Order	O 3123.00	OHRM
NIST Zero Tolerance Harassment Policy	Policy	P 3200.00	CRDO
Identification of Institutional Support Rate Type	Procedure	PR 4000.01	OFRM
Working Capital Fund	Procedure	PR 4100.01	OFRM
Scientific Integrity	Policy	P 5100.00	ADLP
Scientific Integrity	Order	O 5101.00	ADLP
Procedures for Reporting and Resolving Allegations Regarding Violations of Scientific Integrity	Procedure	PR 5101.01	ADLP
Responsible Conduct of Research	Policy	P 5200.00	ADLP
Responsible Conduct of Research Order	Order	O 5201.00	ADLP
Procedures in Response to Allegations of Research Misconduct	Procedure	PR 5201.01	ADLP
Participation in Documentary Standards Activities	Policy	P 5300.00	SCO
Participation in Documentary Standards Activities	Order	O 5301.00	SCO
Measurement Quality	Policy	P 5400.00	SCO
Human Subjects Protections	Policy	P 5500.00	HSPO
Human Subjects Protection Program	Order	O 5501.00	HSPO
Human Subjects Protection Program Procedures	Procedure	PR 5501.01	HSPO
Standard Reference Materials Program	Policy	P 5600.00	ADLP
Standard Reference Materials Program	Order	O 5601.00	ADLP
Managing Public Access to Results of Federally Funded Research	Policy	P 5700.00	ADLP
Managing Public Access to Results of Federally Funded Research	Order	O 5701.00	ADLP
U.S. Designated Institutes Participating in the Mutual Recognition Arrangement (CIPMMRA)	Policy	P 5810.00	ADLP
U.S. Designated Institutes Participating in the Mutual Recognition Arrangement (CIPMMRA)	Order	O 5810.00	ADLP
Calibration Services	Policy	P 5900.00	PML
Calibration Services Order	Order	O 5901.00	PML
Establishment of Calibration Services	Suborder	S 5901.01	PML
Determining and Setting Calibration Fees	Suborder	S 5901.02	PML
Significant Changes to a NIST Calibration Service	Suborder	S 5901.03	PML
Termination of a Calibration Service	Suborder	S 5901.04	PML
Information Systems Management and Use Policy	Policy	P 6100.00	OISM
Employee-Issued Computing and Telecommunications Devices	Notice	N 6100.01	OISM

NIST DIRECTIVES INVENTORY

Title	Type	Number	OU
Network - Boundary Protection	Suborder	S 6102.01	OISM
Basic Input/Output System (BIOS)	Suborder	S 6102.04	OISM
Network - External Connections	Suborder	S 6102.06	OISM
Network - Wireless Security (IEEE 802.11)	Suborder	S 6102.07	OISM
Vulnerability Scanning	Suborder	S 6102.09	OISM
Cybersecurity Workforce	Suborder	S 6102.13	OISM
Information System Vulnerability Management	Suborder	S 6102.15	OISM
Privacy Data Loss Prevention	Suborder	S 6102.16	OISM
Web-Based Voice/Video Conferencing Services and/or Software Product Use	Suborder	S 6102.18	OISM
Information System Contingency Plan Testing	Suborder	S 6102.25	OISM
Use of Electronic Signatures	Suborder	S 6102.28	OISM
Access and Use of IT Resources	Order	O 6103.00	OISM
Access and Use of Web-Based Voice/Video Conferencing Services and/or Software Product Use	Notice	N 6103.06	OISM
Access and Use BitTorrent Peer-to-Peer File Sharing	Notice	N 6103.07	OISM
Access and Use of Personal Identity Verification (PIV) Card Authentication to Information Systems	Notice	N 6103.09	OISM
Access and Use of IT While on Foreign Travel	Notice	N 6103.10	OISM
Access and Use of Automatic Email Forwarding	Notice	N 6103.12	OISM
Access and Use of Dropbox	Notice	N 6103.13	OISM
Access and Use of Remote Connection to NIST	Notice	N 6103.14	OISM
Access and Use of Skype	Notice	N 6103.15	OISM
Access and Use of Microsoft Windows 8	Notice	N 6103.20	OISM
Access and Use of Microsoft Windows Vista	Notice	N 6103.21	OISM
Access and Use of Electronic Signatures	Notice	N 6103.22	OISM
Access and Use of Personally Owned Devices	Notice	N 6103.24	OISM
Investigating Suspected Misuse of IT Resources	Order	O 6104.00	OISM
Position Sensitivity Levels for Information System Security	Order	O 6105.00	OISM
Information Technology (IT) Compliance in Acquisition Checklist	Procedure	PR 6106.01	OISM
Management of Windows and Macintosh Computers	Order	O 6110.00	OISM
Occupational Safety and Health	Policy	P 7100.00	OSHE
Occupational Health and Safety Management System	Order	O 7101.00	OSHE
Safety Rights and Responsibilities	Suborder	S 7101.01	OSHE
Employee Reporting of Unsafe or Unhealthful Working Conditions (UWC)	Suborder	S 7101.02	OSHE

NIST DIRECTIVES INVENTORY

Title	Type	Number	OU
Stop Work	Suborder	S 7101.03	OSHE
Safety and Health Requirements for Minors	Suborder	S 7101.04	OSHE
Hazard Review	Suborder	S 7101.20	OSHE
Personal Protective Equipment (PPE)	Suborder	S 7101.21	OSHE
Safety Education and Training	Suborder	S 7101.23	OSHE
Incident Reporting and Investigation	Suborder	S 7101.24	OSHE
NIST Biosafety Suborder	Suborder	S 7101.50	OSHE
Bloodborne Pathogens Suborder	Suborder	S 7101.51	OSHE
Cryogen Safety	Suborder	S 7101.52	OSHE
Magnetic Field Safety Suborder	Suborder	S 7101.53	OSHE
Dispersible Engineered Nanomaterials	Suborder	S 7101.54	OSHE
Hearing Protection	Suborder	S 7101.55	OSHE
Control of Hazardous Energy (Lockout/Tagout) Suborder	Suborder	S 7101.56	OSHE
Permit-Required Confined Spaces	Suborder	S 7101.57	OSHE
Respiratory Protection	Suborder	S 7101.58	OSHE
Chemical Hazard Communication	Suborder	S 7101.59	OSHE
Compressed Gases	Suborder	S 7101.61	OSHE
Office Safety	Suborder	S 7101.62	OSHE
Electrical Safety	Suborder	S 7101.64	OSHE
Ionizing Radiation Safety	Policy	P 7200.00	OSHE
Ionizing Radiation Safety - Radioactive Material and Ionizing-Radiation-Producing Machines	Order	O 7201.00	OSHE
Environmental Management	Policy	P 7300.00	OSHE
Environmental Management	Order	O 7301.00	OSHE
Fire and Life Safety	Order	O 7401.00	OSHE
Fire and Life Safety	Policy	P 7400.00	OSHE
Preparation and Clearance of Federal Interagency and Non-Federal Agreements	Order	O 8103.00	OAAM
Government Purchase Card Program	Order	O 8201.00	OAAM

Forms Management

NIST PR 1000.05
Effective Date: 8/7/2014

PURPOSE

This procedure establishes the responsibilities for the National Institute of Standards and Technology (NIST) Forms Management, as they relate to all forms used at NIST. The objective is to ensure the use of the correct version of approved forms and to increase the effectiveness and availability of forms. This directive replaces Administrative Manual Subchapter 2.05

APPLICABILITY

This directive applies to all NIST forms.

LEGAL AUTHORITIES AND REFERENCES

- [Paperwork Reduction Act \(PRA\) 44 U.S.C. 3501 et seq.](#)
- [Government Paperwork Elimination Act \(GPEA\), P. L. 105-277, Title XVII](#), (beginning on page 750)
- [5 Code of Federal Regulations Part 1320](#), Controlling Paperwork Burdens on the Public
- [41 Code of Federal Regulations Part 102-194](#), Standard and Optional Forms Management
- [Department Administrative Order 205-10](#), Forms Management
- [NIST Notice 6103.22](#) Access and Use of Electronic Signatures

DEFINITIONS

Form - A fixed or sequential order of data elements, independent of presentation media, approved for the collection and/or exchange of information necessary to execute or report Departmental business transactions (mission and support activities) (DAO 205-10).

Forms include but are not limited to letters, postcards, and memoranda, printed or otherwise reproduced with space for filling in information, descriptive material, or addresses. Documents without fill-in space, such as contract provisions, instruction sheets, notices, tags, labels, and posters, may be considered forms when it is advantageous to identify and control them as forms for purposes of reference, printing, stocking, distribution, and use with other forms.

Forms in general use at NIST are identified as the following types (forms are approved for use by the originating agency's Forms Management Officer):

- Standard Form (SF) - A form approved by General Services Administration (GSA) for use by all Federal agencies.

- Optional Form (OF) - A form used by one Federal agency and approved by GSA for optional use by other agencies in lieu of an individual agency form.
- Office of Personnel Management (OPM) – A form created by the Office of Personnel Management for use by all Federal agencies.
- Department of Commerce (CD) - A form approved for general use within the Department of Commerce.
- National Institute of Standards and Technology (NIST) - A form originated and approved for use by the National Institute of Standards and Technology.
- Document Number (DN) - A form originated and approved for use by the National Institute of Standards and Technology. DN forms are usually temporary in nature.
- Boulder (NIST/BL) - A form originated by NIST-Boulder and approved for its use.
- Other-Agency - A form originated within another government office or agency (e.g. Office of Management and Budget (OMB) form, Office of Government Ethics (OGE) form, Internal Revenue Service (IRS) form, etc.) and approved for use by all Federal agencies.

RESPONSIBILITIES

NIST Forms Management Officer

- Manages forms at NIST;
- Approves and takes appropriate action on all requests for new, revised, reprinted, and electronic NIST forms;
- Analyzes and designs forms to improve related procedures and flow of work (Note: routine forms are designed by the NIST Forms Management Program staff; specialty forms may be sent to a contractor for design.);
- Assigns form numbers to all NIST forms,
- Ensures new NIST forms do not duplicate existing standard, optional, OPM, Commerce Department, NIST, or other agency forms;
- Recommends the most efficient and economical methods of reproduction;
- Approves all Forms Management service requests.
 - Gaithersburg requests must be signed and dated by the NIST Forms Management Officer before the request is accepted by the NIST [Facilities Services Division](#);
 - Boulder requests must be signed and dated by the NIST Forms Management Officer before the request is accepted by the NOAA Facilities Operations Division's Publications Branch.
- Maintains a history file for all NIST forms;

- Updates the [NIST Forms Catalog](#) containing form number, form name, revision date, availability, and form owner;
- Processes requests for approval of exceptions to Standard and Optional Forms;
- Approves requests for new and revised stationery and envelopes, assuring that the format complies with [DAO 201-1](#) for the approval and use of seals, emblems, insignia and logos and [Department of Commerce Publishing and Printing Management Manual](#); and
- Notifies NIST Organizational Unit (OU) designated forms contacts by email when NIST, Department of Commerce, Standard, and Optional forms are revised or made obsolete.

NIST OU Directors/Chief Officers/Division Chiefs and Office Directors/Managers

- Ensure each NIST form has a designated owner;
- Ensure NIST forms are properly vetted through required individuals;
- Ensure modifications to existing NIST forms are implemented when necessary; and
- Ensure new NIST forms are created and implemented as required.

NIST Forms Contacts

- Function as their OU contact for all forms related issues; and
- Disseminate forms notifications/information throughout their program area.

NIST Form Owner

- Develops the requirements for their NIST forms;
- Maintains the form template;
- Ensures the accuracy and current status for each form, and informs the NIST Forms Management Officer in a timely manner when changes are required; and
- Coordinates and/or reviews cross-discipline content prior to vetting to ensure consistency with other directives' content.

NIST Facilities Services Division

- Returns to the NIST Forms Management Officer all requests for forms (numbered or unnumbered, NIST or other agency) that have not been approved (signed and dated) by the NIST Forms Management Officer; and
- Processes requests from the NIST Forms Management Officer for all forms printing.

Information Technology Assistance Center (ITAC)

- Provides service and installation of OISM-supported forms software.

PROCEDURE

Request for development of a new form, revisions to an existing form, or print hard copies of new or existing forms:

- Send all requests for new or revised forms to the Forms Management Officer:
 - Mail stop 1711; or
 - Email attachment to donna.miller@nist.gov; or
 - Through eApproval
- Complete forms NIST-66 Request for Forms Management Services and NIST-223 Requisition for Duplicating Services, (NIST-223 needed only for forms to be printed), and forward along with form changes, sample/draft of new or revised form and/or description of purpose and content to be collected.
- NIST Forms Management Officer returns completed draft to form owner for approval.
- Approved form is posted on the [NIST Online Forms](#) page by the NIST Forms Management Officer.

DIRECTIVE OWNER

101 - Management and Organization Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	2/8/2013	Donna Miller	Draft Document
Rev. .01	4/5/2013	Donna Miller	Updated with comments from M&O
Rev. .02	6/27/2013	Donna Miller	Updated with Comments from Mike Herman
Rev. .03	1/8/2014	Donna Miller	Updated based on OCC Comments
Rev. .04	2/2/2016	Dan Cipra	Incorporated all OCC comments

NIST Administrative Committees

NIST O 1005.00
Effective Date 04/03/2014

PURPOSE

This directive establishes the requirements, roles and responsibilities for the creation, maintenance and termination of all NIST administrative committees in accordance with the requirements of NIST leadership and organizations.

APPLICABILITY

This directive is applicable to all NIST employees.

This directive does not apply to:

- Any voluntary employee organization or group, including but not limited to SEBA, Toastmasters, and Photography.

REFERENCES

- Department of Commerce Administrative Order 200.00 Handbooks and Manuals
- Administrative Manual 2.06 – Records Management

REQUIREMENTS

- NIST shall create and maintain effective and efficient administrative committees to assist in carrying out NIST's programmatic and administrative functions.
- Each administrative committee shall function within the scope of a formally defined, approved and maintained charter. At a minimum, the charter must contain the following sections (See Appendix A for a sample charter template).
 - Background
 - Objectives
 - Membership
 - Official to Whom the Administrative Committee Reports
 - Operating Principles/Administration
 - Meeting Policies
 - Revisions of the Charter
- Only Federal employees may serve as administrative committee members with the exception of Editorial Review Boards whose members, selected by Organizational Unit (OU) Directors, may be retired NIST staff members.

- Records and files of the administrative committee shall be maintained and handled in accordance with Administrative Manual 2.06 Records Management. The Chairperson of each administrative committee shall be responsible for the records and files of the committee.
- All requests to establish an administrative committee shall be routed to the Management and Organization Office by the sponsoring Associate Director (AD).
- All new administrative committee requests shall be prepared in memorandum format for presentation to the NIST Director. If the Director gives preliminary approval, the requesting official may be asked to make a presentation to the NIST Leadership Board.
- All requests to terminate an administrative committee shall be approved by the NIST Director. The sponsoring AD must send a memorandum requesting termination to the Management and Organization Office for routing through appropriate NIST officials to the NIST Director.

DEFINITIONS

Administrative Committee – A body of federal NIST employees (with the exception of the Editorial Review Boards) delegated authority to consider, investigate, recommend, take action on, or report on some NIST administrative matter.

RESPONSIBILITIES

NIST Director

- Approves the creation and termination of NIST administrative committees and appoints all administrative committee members.
- Approves administrative committee charters and revisions thereto.

NIST Associate Directors

- Review all NIST administrative committee charters and revisions thereto.
- Submit draft charters for new administrative committees and requests for termination of existing administrative committees to the Management & Organization Office.

Office of the Chief Counsel for NIST

- Review all NIST administrative committee charters and revisions thereto.

Administrative Committee Chairperson

- Submits revisions to the administrative committee's charter to the Management and Organization Office for routing through appropriate NIST officials to the NIST Director for approval

- Maintains proper records and files, including:
 1. Administrative Committee roster
 2. Record of administrative committee activities (agendas and minutes)

Management and Organization Office

- Routes all draft charters for new administrative committees, revisions to charters for existing administrative committees, and requests to terminate administrative committees through appropriate NIST officials to the NIST Director for approval.
- Coordinates with the chairperson or designee to ensure a review cycle for the charter.
- Provides advice and consultation during the charter drafting process, as needed.
- Publishes and maintains administrative committee information on the NIST Internal Website.
- Maintains the official list of NIST administrative committees and the approved administrative committee charters.

DIRECTIVE OWNER (DO)

101 - Management and Organization Office (M&O)

APPENDICES

- A. Administrative Committee Charter Template
- B. Revision History

APPENDIX A

ADMINISTRATIVE COMMITTEE CHARTER TEMPLATE

_____ Administrative Committee Charter

Submitted by: _____
NIST Official requesting to establish an
Administrative Committee _____
Date

Reviewed by: _____
Office of the Chief Counsel for NIST _____
Date

Reviewed by: _____
Associate Director for Innovation and
Industry Services _____
Date

Reviewed by: _____
Associate Director for Management Resources _____
Date

Reviewed by: _____
Associate Director for Laboratory Programs _____
Date

Approved by: _____
NIST Director _____
Date

MM/DD/YYYY**AUTHORITY (*Optional*)**

As needed.

BACKGROUND (*Mandatory*)

This section will be used to describe the administrative committee or the events that led up to the creation of the administrative committee. It can contain historical information, decision points or anything that will aid the reader and shed more light on the administrative committee.

OBJECTIVES (*Mandatory*)

This section will spell out the goals and objectives of the administrative committee. It is best done in a series of bullet statements using action words as shown below.

- Supporting the
- Providing a forum for, and
- Recommend possible solutions to the NIST Director and Associate Directors on

MEMBERSHIP (*Mandatory*)

This section will list the members of the administrative committee by title and their Organizational Units.

Members (Organizational Unit - OU) (*Mandatory*)

Position Title - OU Name (###)

Chair (*Mandatory*)

List the organization and/or role that will serve as chair.

Designated Representatives (*Optional*)

Any member may designate another appropriate federal employee to represent the member's organization on the _____, provided that the member has delegated to that individual the authority to represent fully the interests of the member's organization in the conduct of _____ business.

Qualifications (*Optional*)

List any specific requirements or capabilities the members must have.

**OFFICIAL TO WHOM THE ADMINISTRATIVE COMMITTEE REPORTS
(*Mandatory*)**

List the NIST official to whom the administrative committee reports.

SUPPORT (*Mandatory*)

_____ will serve as Secretary. The Secretary shall be responsible at the discretion and direction of the Chair, for maintaining the agenda, distributing materials in advance of meetings, maintaining and distributing minutes of meetings, tracking board assignments and actions as needed, and performing other operational duties.

OPERATING PRINCIPLES/ADMINISTRATION (*Mandatory*)

This is where the actual purpose and duties of the administrative committee are spelled out. They can be described in a paragraph or listed as bullets.

RESPONSIBILITIES (*Optional*)

This section could be used to list the specific responsibilities of the administrative committee or of specific members of the administrative committee or positions on the committee, held by members of the committee.

ESTIMATED OPERATING COSTS (*Optional*)

List any costs as necessary (e.g., labor costs, meeting costs, travel, etc.).

MEETING POLICIES (*Mandatory*)

Frequency (*as applicable*)

List how often the administrative committee will convene.

Agendas (*as applicable*)

List how the administrative committee will manage the agenda.

Attendance (*as applicable*)

This section is to describe if there are any requirements as to minimum number of attendees and any special rules.

Minutes and Action Items (*as applicable*)

List how the administrative committee will manage the minutes.

Decision Making

What constitutes a quorum for decision making?

Will the administrative committee vote to make decisions? If so, what constitutes a passing vote?

Must votes be taken in person?

SUBCOMMITTEES AND WORKING GROUPS (*Optional*)

The _____ may establish and dissolve subcommittees and working groups under the jurisdiction of the _____ and deemed necessary for the _____ to advance its goals and objectives.

REVISIONS OF THE _____ CHARTER (*Mandatory*)

The _____ Chair, on behalf of the _____, shall propose revisions to the _____ charter to the NIST Director as necessary to ensure that it accurately reflects the Board's objectives and operations. All charter revisions must be approved by the NIST Director.

DURATION/TERMINATION (*Optional*)

List the information as required

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	1/30/13	Dan Cipra	Initial draft
Rev 1.01	2/22/16	Dan Cipra	Updated Directive Number

Organizational Changes

NIST O 1007.00
Effective Date: 3/13/2013

PURPOSE

This directive sets the requirements and responsibilities for requesting and making organizational changes at NIST. This document partially replaces NIST Administrative Manual Subchapter 9.03 of the same name; the procedures portion will be addressed in a separate directive.

APPLICABILITY

This directive applies to NIST-Gaithersburg and NIST-Boulder, specifically to all organizational changes requiring DOC and/or NIST approval.

REFERENCES

- [Department of Commerce Administrative Order \(DAO\) 200-7, Department Organization Order Series](#)
- [Department of Commerce Organizational Order \(DOO\) 30-2B, National Institute of Standards and Technology](#)

REQUIREMENTS

All NIST functions shall be organized and staffed in the most economical manner consistent with effective program accomplishment and with sound organizational planning criteria.

All organizational changes which affect DOO 30-2B must be approved by the Under Secretary of Commerce for Standards and Technology/NIST Director, and the Department of Commerce (DoC) Chief Financial Officer and Assistant Secretary for Administration.

The authority to implement an organization management system at NIST is prescribed in DAO 200-7, and delegates authority to the Under Secretary of Commerce for Standards and Technology/NIST Director to approve changes to organizational structures not requiring changes to the Department of Commerce Organizational Order (DOO) 30-2B, i.e. divisions, offices, and groups below the Organizational Unit (OU) level.

DEFINITIONS

Associate Director (AD) – For purposes of this directive, the level of the NIST organization that is directly below the NIST Directors office. ADs report to the NIST Director and are also considered an OU.

Division/Office – For purposes of this directive, the level of the NIST organization that is directly below the OU level. An OU is not required to have Divisions/Offices. Divisions/Offices report to the OU level Director.

DOO 30-2B - Prescribes the organizational structure and assignment of functions within NIST. NIST organizational changes requiring Departmental approval are formally requested and approved through the process for revising DOOs, set forth in DAO 200-7. Changes which may affect DOO 30-2B include organizational changes:

- For the Operating Unit level, (i.e. NIST)
- For the Associate Directorate level, and
- For organizational units reporting to the NIST Director or Associate Directors

Group - For purposes of this directive, the level of the NIST organization that is directly below the Division/Office level. Groups report up to the Division/Office level. For OUs that do not have Divisions/Offices, Groups report to the OU level Director.

Office – See Definition for Division/Office.

Organization Management System – Describes the arrangement of functions into a formal organizational structure including OU, and levels below the OU level, i.e. divisions, offices, and groups.

Organizational Change -

- 1) Creation, abolishment, transfer, or consolidation within an OU;
- 2) Changes in the name or code number within an OU;
- 3) Adoption, termination, or modification of a function within an OU;
- 4) Transfer of a function or portion of a function across organizational lines, across OUs, divisions, offices and/or groups, including the transfer of full-time equivalents (FTEs), base appropriated/institutional support funds, and/or equipment related to the transfer of a function; or
- 5) Action to eliminate duplication of a function of another OU.

Organizational Unit (OU) – For purposes of this directive, the highest level in the NIST organization. Each OU is headed by an OU Director that reports to one of the three NIST Associate Directors. Associate Directors report to the NIST Director.

RESPONSIBILITIES

Under Secretary of Commerce for Standards and Technology/NIST Director:

- Establishes the objectives and requirements of the organization management system at NIST;
- Approves organizational change requests affecting DOO 30-2B before routing to the DoC Chief Financial Officer and Assistant Secretary for Administration for approval; and

- Approves NIST organizational changes below the level affecting DOO 30-2B.

Associate Directors:

- Ensure effective operation within their directorate, and
- Approve organizational change requests before routing to the Under Secretary of Commerce for Standards and Technology/NIST Director for approval.

Organizational Unit Directors:

- Ensure effective operations within their OU; and
- Request approval for organizational changes through their Associate Director.

Management and Organization Office:

- Coordinates the planning, approval, and implementation process for organizational changes for NIST;
- Provides consulting services to NIST officials who propose to make organizational changes;
- Reviews organizational change proposals to ensure compliance with established guidelines on organizational structure and nomenclature;
- Coordinates the implementation date with representatives from the Office of the Director, Office of Financial Resource Management, Office of Workforce Management, Office of Facilities and Property Management, Office of Information Systems Management, and the OU requesting the change;
- Retains supporting information, such as the explanation of the proposed change, functional statements, budget and staffing impact statements, and related organizational charts;
- Coordinates and controls required documentation for review, clearance, and approval, including revisions or amendments to DOO 30-2B;
- Secures approval from the appropriate Associate Director, Under Secretary of Commerce for Standards and Technology/NIST Director and the DoC Chief Financial Officer and Assistant Secretary for Administration as needed; and
- Tracks all organizational change proposals through the clearance process within the DoC.

Office of Workforce Management:

- Reviews the organizational change proposal and clears the staffing impact statement. (The staffing impact statement is required for all reorganization requests at both the OU level, which requires DoC approval, and for those below the OU level (division, office, and group) that do not require DoC approval.)
- The review of the organizational change proposal must consider the impact on:

- 1) Staffing requirements including series/grades/pay bands;
- 2) P.L. 3104 and SES positions, if any are involved; and
- 3) Ramifications of possible adverse impact on employees.

Office of Financial Resource Management

Budget Division:

- Reviews the organizational change proposal and clears the budgetary impact statement. (The budgetary impact statement is required for all reorganization requests at both the OU level, which requires DoC approval, and for those below the OU level (division, office, and group) that do not require DoC approval.)
- The review of the organizational proposal must consider the impact on:
 - 1) Current year and next fiscal year budgets;
 - 2) Justification and explanation of how any increased costs, if applicable, will be funded or defrayed; and
 - 3) Approval of assigned organizational code numbers.
- Prepares a notification of reprogramming and/or reorganization from the NIST Director to the Chief Financial Officer and Assistant Secretary for Administration, which discusses any significant programmatic effects of the proposed organizational change for those reorganizations that require DoC approval.

Finance Division:

- Reviews the organizational change proposal and considers the impact on:
 - 1) Internal and external financial reporting systems;
 - 2) Transfer of recorded obligations accurately and in a timely manner;
 - 3) Accurate recording of new obligations;
 - 4) Transfer of reimbursable agreement information with accurate recording of new and existing unfilled customer orders in a timely manner;
 - 5) Coordination of internal reporting change; and
 - 6) Transfer of funding sources.
- Implements actions once the reorganization has been approved.

Office of Information Systems Management:

- Reviews the organizational change proposal and considers the impact on:
 - 1) IT system privileges and resources, and local IT management responsibilities;
 - 2) Data ownership and data migration;

- 3) Proposed changes on existing OU-specific Service Agreements; and
 - 4) Network and telecommunications changes related to relocation of staff and equipment.
- Implements actions once the reorganization has been approved.

Office of Facilities and Property Management:

- Reviews the organizational change proposal and considers the impact on space if OU requests additional or contiguous space; and
- Oversees and assists the implementation of personal property reassignments once OU/Division reorganizations have been approved.

APPROVAL AND IMPLEMENTATION DATES OF CHANGES

For organizational changes which affect DOO 30-2B, the approval date is the effective date of the revised DOO 30-2B.

For organizational changes which do not affect DOO 30-2B, the approval date is the date the change is approved by the NIST Director.

- The implementation date for the organizational change is coordinated by the Management and Organization Office with the affected OU and those offices (Office of Financial Resource Management, Office of Workforce Management, Office of Facilities and Property Management, and the Office of Information Systems Management) responsible for implementation. The use of new or changed organizational names and code numbers is not permitted until the implementation date.

DIRECTIVE OWNER

101 - Management and Organization Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/12/2012	Dan Cipra (M&O)	First Draft
Rev. 1.01	11/15/2015	Dan Cipra	Updated links

Contacts with Members of Congress, Congressional Committees, their respective staffs or the Congressional Research Service, and Intergovernmental entities including State, county, municipal governments and their associations (local governments)

NIST O 1030.00
Effective Date: 6/25/2014

PURPOSE

To define NIST requirements and responsibilities regarding contacts on official business with Members of Congress, Congressional Committees, their respective staffs or the Congressional Research Service (CRS), and Intergovernmental entities including State, county, municipal governments and their associations (local governments) (referred hereafter as “the group”). This directive replaces Administrative Manual Subchapter 4.06.

APPLICABILITY

This directive applies to NIST employees that contact or receive contact from “the group” related to any official NIST work/business issues. This directive does NOT apply to communications to/from “the group” that fall under the whistleblower protection laws.

LEGAL AUTHORITIES AND REFERENCES

- [18 U.S.C. 1913 - Lobbying with Appropriated Moneys](#)
- [Department Administrative Order 218-1, Legislative Activities](#)
- [Department Administrative Order 218-2, Legislative and Intergovernmental Affairs](#)
- [Department Organization Orders 20-3, Director for Budget](#)
- [5 U.S.C. § 7211](#), Employees’ right to petition Congress (governing disclosures to Congress)
- [5 U.S.C. § 2302\(b\)\(8\)](#), as amended by the Whistleblower Protection Act of 1989 and Whistleblower Protection Enhancement Act of 2012 (governing disclosures of violations of any law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety)

REQUIREMENTS

NIST Congressional and Legislative Affairs Office

- The NIST Congressional and Legislative Affairs (CLAO) Office will provide a prompt response to contacts by “the group”.
- All incoming mail from “the group” shall be forwarded to the NIST CLAO and shall be answered either
 - a) Within seven (7) business days after the date it is received or
 - b) On the date assigned by the Department Executive Secretariat (Exec Sec) or NIST Exec Sec.

Employees

- Employees must immediately inform the NIST CLAO Director (or a representative) of all contacts from “the group”.
- Employees shall NOT contact any individual of “the group” regarding NIST official work/business related issues until NIST CLAO is formally notified and a determination regarding the appropriate response is defined.

DELEGATION OF AUTHORITY

- The NIST Chief Facilities Management Officer (FMO) is delegated authority to sign responses to inquiries regarding all matters within the Office of Facilities and Property Management’s (OFPR) purview including, but not limited to, facility matters.
- The NIST Chief Financial Officer (CFO) is delegated authority to sign responses to inquiries regarding all matters within the Office of Financial Resource Management’s (OFRM) purview including, but not limited to, budget and finance.
- The NIST Chief Information Officer (CIO) is delegated authority to sign responses to inquiries regarding all matters within the Office of Information Systems Management’s (OISM) purview including, but not limited to, NIST information security policies.
- The NIST Chief Safety Officer (CSO) is delegated authority to sign responses to inquiries regarding all matters within the Office of Safety, Health, and Environment’s (OSHE) purview including, but not limited to, safety, health, and environmental matters.
- The NIST Office of Acquisition and Agreements Management (OAAM) Director is delegated authority to sign responses to inquiries regarding all matters within the Acquisition and Grants Management Divisions’ and the Reimbursable Agreements Coordination Office’s purview including, but not limited to, financial assistance awards (grants/cooperative agreements), procurement matters, and reimbursable agreements.

- The NIST Office of Human Resources Management (OHRM) Director is delegated authority to sign responses to inquiries regarding all matters within the OHRM, including, but not limited to, employment and personnel matters.

Receipt and Distribution of Mail from “the group”

Upon receipt of correspondence from “the group,” addressee shall immediately contact the NIST CLAO and provide a copy. If a response is required, the NIST Exec Sec will enter the correspondence into the official NIST Control process, and a control ticket will be assigned to the appropriate office to prepare a response.

Signature Authorities

Official Inquiries

- Responses to legal, legislative, and politically sensitive matters are signed by the NIST Director/Under Secretary of Commerce for Standards and Technology. After the reply has been drafted by the assignee and received the concurrence of the Organizational Unit (OU) Director, the undated response shall be routed through the Chief Counsel (CC) for NIST, the NIST CLAO Director, the NIST Chief of Staff (CoS), and the appropriate Associate Director (AD) as it relates to the subject matter (AD for Laboratory Programs (LP), AD for Innovation and Industry Services (IIS), or AD for Management Resources (MR)) then to the Office of the Director for signature. The NIST CLAO will be responsible for dispatch.
- Responses to specialized/specific inquiries are signed by the NIST CLAO Director. After concurrence by the OU Director, the undated response shall be routed through the CC for NIST, the NIST CLAO Director, the NIST CoS for concurrence, and the appropriate AD as it relates to the subject matter (AD for LP, AD for IIS, or AD for MR) then back to the NIST CLAO for signature, dating and dispatch.
- Responses to employment and personnel matters related to NIST are signed by the Director, NIST OHRM. The signed, undated response shall be routed through the CC for NIST, the NIST CLAO Director, the NIST CoS, and the appropriate AD as it relates to the subject matter (AD for LP, AD for IIS, or AD for MR) for concurrence, then back to the NIST CLAO for dating and dispatch. Responses to administrative matters (for example, facilities, budget, procurement, information security policies, safety) are signed by the respective Office Director or Chief Officer (Director, Office of Acquisition and Agreements Managements, Director, OHRM, CFO, CIO, CSO, or CFM Officer). The signed, undated response shall be routed through the CC for NIST, the NIST CLAO Director, the NIST CoS, and the appropriate AD as it relates to the subject matter (AD for LP, AD for IIS, or AD for MR) for concurrence, then back to the NIST CLAO for dating and dispatch.

Exempt Inquiries

- Communications from a member of “the group” addressed to a staff member by name, which is found by the addressee to be personal and not related to official NIST or Department of Commerce (DoC) business, is exempt from the requirements of this directive.
- Communications to/from the group that fall under laws permitting specified disclosures are exempt from this directive:
 - i. Under 5 U.S.C. § 7211, titled “Employees’ right to petition Congress,” “The right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied.”
 - ii. 5 U.S.C. 2302(b)(8), as amended by the Whistleblower Protection Act of 1989 and Whistleblower Protection Enhancement Act of 2012, protects any disclosure of information by an employee or applicant that an employee or applicant reasonably believes evidences any violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

Correspondence Procedures

If the subject of the individually addressed correspondence is official business, the reply shall be handled as follows:

- If the response involves a programmatic matter within the field of competence of the addressee, they shall advise the NIST CLAO and provide a copy of the incoming letter to the NIST CLAO. The NIST CLAO will review and provide instructions to the NIST Exec Sec, who will log in and prepare a control ticket for correspondence package. The control ticket will provide the due date, name of individual signing correspondence, and clearing routing instructions. Clearances shall include their respective OU Office, CC for NIST, the NIST CLAO Director, the NIST CoS, and the appropriate AD as it relates to the subject matter (AD for LP, AD for IIS, or AD for MR) for concurrence, and then back to the NIST CLAO for dating and dispatch.
- If the response involves a programmatic matter not within the field of competence of the addressee, the addressee shall immediately advise the NIST CLAO. The NIST CLAO will advise the NIST Exec Sec. The NIST Exec Sec will assign the correspondence to the appropriate OU for reply. An information copy of the reply shall be prepared for the NIST staff member who received the personally addressed inquiry. Clearances shall include the OU Office assigned, CC for NIST, the NIST

CLAO Director, the NIST CoS, and the appropriate AD as it relates to the subject matter (AD for LP, AD for IIS, or AD for MR) for concurrence, and then back to the NIST CLAO for dating and dispatch.

Reporting Inquiries To/From “the group” to the DoC

- Mail/Email Inquiries - The NIST CLAO Director, or designee, reviews the information copies of all correspondence addressed to “the group” and reports contacts to the Department Office of Legislative and Intergovernmental Affairs. NIST CLAO Director, or designee, shall be notified within 1 day after receipt of mail/email inquiry.
- Telephone Contacts - Each staff member who talks to “the group” on NIST official business must report the details of the conversation to the NIST CLAO Director, or designee within 24 hours of the contact.

Copy Requirements for Mail from “the group”

In addition to the Official File Copy, the following copies are required for correspondence: A copy of the signed original incoming letter and a copy of the signed original outgoing response are prepared for each letter addressee, for the NIST Director of CLAO, and for the NIST Exe Sec. The copies are distributed by the NIST Exec Sec.

RESPONSIBILITIES

NIST CLAO Director

- Coordinates all NIST contacts with “the group” and is responsible for reporting inquiries and requests from “the group” to the NIST Director/Under Secretary of Commerce for Standards and Technology and to the Assistant Secretary of Commerce for Legislative and Intergovernmental Affairs.
- Designates a CLAO representative or accompanies all NIST officials on any visits, unless it is mutually agreed, in advance, that such accompaniment is unnecessary.
- Reports and coordinates responses to inquiries on legislation with the appropriate NIST officials and the DoC (Department)'s General Counsel, who ensures that the response is coordinated within the Department.
- Works with senior NIST leaders to develop and execute responses to appropriation and related funding inquiries. CLAO will coordinate with the NIST Budget Division, which will coordinate the response with the DOC Director of the Office of the Budget in accordance with DOO 20-3, Director for Budget, section 3.a.

OU Directors

- Seek the advice of the NIST CLAO when an inquiry is received from “the group”.

- Inform and consult with the NIST CLAO, who will advise NIST management prior to any scheduled visits with or calls to “the group”, whether requested by the outside organization or initiated by NIST officials.

NIST Exec Sec

- Maintains a log system for mail and distributes information copies to appropriate NIST officials.

NIST Employees

- Follow the procedures in this directive concerning contact with “the group” on official matters.
- Inform and consult with the NIST CLAO prior to any scheduled visits with or calls to “the group”, whether requested by the outside organization or initiated by NIST officials

DIRECTIVE OWNER

111 – Congressional and Legislative Affairs Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/29/2012	Kandy Hauk	Initial Draft
Rev. .01	8/30/2012	Dan Cipra	Formatting changes only
Rev. .02	10/22/12	Kandy Hauk	Provided updates
Rev. .03	12/28/12	Kandy Hauk	Addressed M Lieberman's comments
Rev. .04	1/15/13	Kandy Hauk	Addressed M Lieberman's comments
Rev. .05	1/17/13	Kandy Hauk	Incorporated Heather Evans and Linda Acierto's comments/edits
Rev. .06	11/27/13	Kandy Hauk	Addressed M Lieberman's comments
Rev. .07	1/8/14	Kandy Hauk	Addressed M Lieberman's comments
Rev. .08	3-18-14	Kandy Hauk	Removed Appendix regarding lobbying
Rev. .09	3/31/14	Dan Cipra	Edits from OCC incorporated.
Rev. .10	4/23/14	Kandy Hauk	Addressed DRB edits
Rev. .11	4/30	Dan Cipra	Accepted all DRB track changes and finalized formatting.
Rev..12	5/12	Kandy Hauk	Address M. Lieberman's comments/edits

Procedures for Transmittal of Federal Advisory Committee Reports to Congress

NIST PR 1030.01
Effective Date: 12/23/2014

PURPOSE

This directive contains the procedures for transmittal of a statutorily mandated Federal Advisory Committee Report to Congress, which is produced by a Federal Advisory Committee chartered to advise the National Institute of Standards and Technology (NIST).

APPLICABILITY

This directive is applicable to all reports statutorily required to be submitted to Congress by a Federal Advisory Committee chartered to advise NIST.

BACKGROUND

All Federal Advisory Committee reports required by statute to be submitted to Congress must be sent to the NIST Congressional and Legislative Affairs Office (CLAO) to manage the required delivery process prior to the report being released.

Please note Federal Advisory Committee reports DO NOT require clearance by NIST, the Department of Commerce (DOC), or the Office of Management and Budget prior to delivery to the Director of NIST, the Secretary of Commerce, or Congress. NIST CLAO will prepare the proper transmittal package to be delivered to either the NIST Executive Secretariat for the NIST Director's signature or to the DOC Executive Secretariat for the Secretary's signature before the report can be submitted to Congress. This transmittal package includes the letters to Congress as required by law.

RESPONSIBILITIES

The Director (or designee) of the Congressional and Legislative Affairs Office (CLAO)

- Ensures that each Federal Advisory Committee has assigned a NIST employee to serve as a Point of Contact (POC).
- Ensures that the report submitted by the Federal Advisory Committee is received from the NIST POC and the appropriate transmittal package is prepared for the signature of the Director of NIST or the Secretary of Commerce depending upon the legislative requirement.
- Notifies the POC for the Advisory Committee and the Director of the respective OU of the official delivery of the report to Congress and that the report may be made publicly available.

The assigned NIST POC for each Federal Advisory Committee

- Receives the report from the Federal Advisory Committee and delivers it to CLAO for transmittal package preparation and routing for clearance.
- Receives notification from CLAO once report is officially delivered to Congress and informs Federal Advisory Committee that transmittal has been completed.

PROCEDURES

The general flow of the process is captured in Appendix A.

1. NIST CLAO receives the Federal Advisory Committee report from the appropriate NIST POC.
2. NIST CLAO prepares the appropriate transmittal package to Congress for the signature of either the Director of NIST or the Secretary of Commerce, which is specified in the statute that mandates the report.
3. NIST CLAO determines which NIST officials must clear each report and obtains the clearances of those officials on the transmittal letter ONLY (NIST is NOT authorized to edit a Federal Advisory Committee's report); this may include the Chief Counsel for NIST, Director of Program Coordination Office, Budget Officer, Chief of Staff, and the respective Associate Director and Director of NIST. NIST CLAO adjudicates any edits and/or comments received and revise appropriately.
4. After NIST clearance and signature of the transmittal letter,
 - a. the NIST CLAO transmits the report to Congress, if signed by the NIST Director, or
 - b. the NIST CLAO sends the transmittal package to the DOC Executive Secretariat for the Secretary of Commerce's signature. After the Secretary of Commerce signature is obtained, the package is delivered to the DOC Office of Legislative and Intergovernmental Affairs for delivery to Congress.
5. After the report has been delivered to Congress, it may be publically released. NIST CLAO coordinates with NIST Public Affairs Office (PAO) and confirms with the POC and the respective OU Director that the report has been delivered to Congress prior to public release.

DIRECTIVE OWNER

111 – Congressional and Legislative Affairs Office (CLAO)

APPENDICES

Appendix A: Process Flow Diagram

Appendix B: Revision History

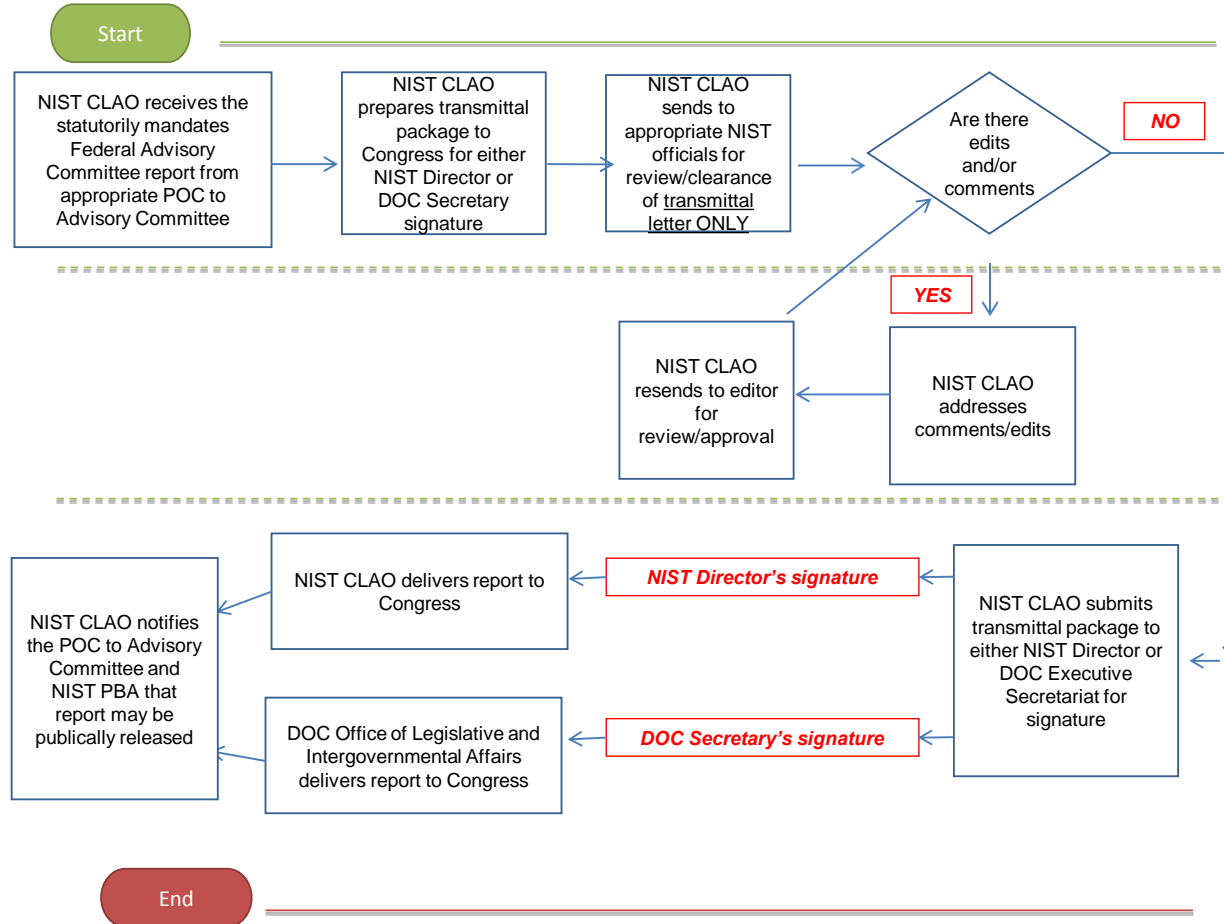
APPENDIX A

PROCESS FLOW DIAGRAM

General Process Flow in relation to:

Reports to Congress required under a law by a Federally Chartered Advisory Committee

as of 3/30/2015



APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/4/2012	Kandy Hauk	First Draft
Ver .01	9/5/2013	Dan Cipra	Formatting changes only
Ver .02	8/29/2014	Kandy Hauk	Edited
Ver .03	11/20/2014	Dan Cipra	Formatting changes only
Ver.04	12/2/2014	Kandy Hauk	Addressing DRB comments
Ver.05	3/11/2015	Kandy Hauk	Addressing Legal comments/edits

Clearance for Reports to Congress - Authorization

NIST PR 1030.02
Effective Date: 12/23/2014

PURPOSE

This directive contains Reports clearance procedures for reports required under an Authorization Law applicable to the National Institute of Standards and Technology (NIST).

APPLICABILITY

The directive is applicable to all reports produced by NIST and required under an Authorization Law to be sent to Congress.

REFERENCES

- [Office of Management and Budget Circular No. A-19](#)
- [Department of Commerce Organization Order \(DOO\) 10-6](#)

BACKGROUND

All reports required by Congress within a Public Law, specifically an Authorization Law, need to be sent to the NIST Congressional and Legislative Affairs Office (CLAO) to manage the required clearance process prior to being released. An Authorizations act is a law that establishes or continues one or more Federal agencies or programs, establishes the terms and conditions under which they operate, authorizes the enactment of appropriations, and specifies how appropriated funds are to be used.

Please note that all reports to Congress must be officially cleared through the various officials at NIST, and then the Department of Commerce (DOC) and the Office of Management and Budget (OMB), and “transmitted” to the legislatively required Congressional Committees/Subcommittees before the report can be publicly released.

RESPONSIBILITIES

The Director (or designee) of the Congressional and Legislative Affairs Office (CLAO)

- Manages the clearance process prior to the document being released.
- Notifies the appropriate the Organizational Unit (OU) of the responsibility of the report and the required due date.

PROCEDURES

The general flow of the clearance process is listed below.

1. NIST CLAO will reach out to the OU Director or appropriate NIST manager to advise of the report requirements and determine appropriate person to be designated to author the report and advise them of the responsibility of the report, the scope, and date due to the NIST CLAO.
2. Final Draft of required report to Congress is prepared by the designated person and cleared through the respective OU prior to being sent to the NIST CLAO (*due 30 days prior to date due to Congress unless instructed otherwise*).
3. After NIST CLAO receives the Final Draft report, NIST CLAO will develop a clearance plan and route to the appropriate NIST officials for clearance; this may include the NIST Chief Counsel, Director of Program Coordination Office, Director of Budget Office, Chief of Staff, and the respective Associate Director and Director of NIST. NIST CLAO will adjudicate any edits and/or comments received and revise appropriately.
4. After NIST clearance is completed, the NIST CLAO will send the report to the DOC Office of General Counsel (OGC). The OGC will send the report to the appropriate DOC officials for clearance; this may include the Office of Budget, Office of Policy and Strategic Planning, Office of Legislative and Intergovernmental Affairs, and the Office of Public Affairs and other DOC agencies. If comments/edits are received, the NIST CLAO will coordinate the response with the author of the report and work to resolve the issues. When DOC approves report, the report will be sent by DOC OGC to OMB for clearance.
5. OMB will send the report out to the Departments within the Federal Government for review. If comments/edits are received, the comments/edits are returned to the DOC OGC which in turn will contact the NIST CLAO to coordinate the response. At that time the NIST CLAO will contact the author of the report to discuss the edits/comments received. After edits/revisions are made and the report clears, DOC OGC will in turn send to OMB for final review and clearance. When OMB approves report, the NIST CLAO will notify the author of the clearance of the report and will prepare the transmittal package to Congress.
6. After the report has been delivered to Congress, it may be publically released. NIST CLAO coordinates with NIST Public Affairs Office (PAO) and will confirm with the author and OU Director or appropriate NIST manager that the report has been delivered to Congress prior to public release.

DIRECTIVE OWNER

111 – Congressional and Legislative Affairs Office (CLAO)

APPENDICES

Appendix A: Process Flow Diagram

Appendix B: Revision History

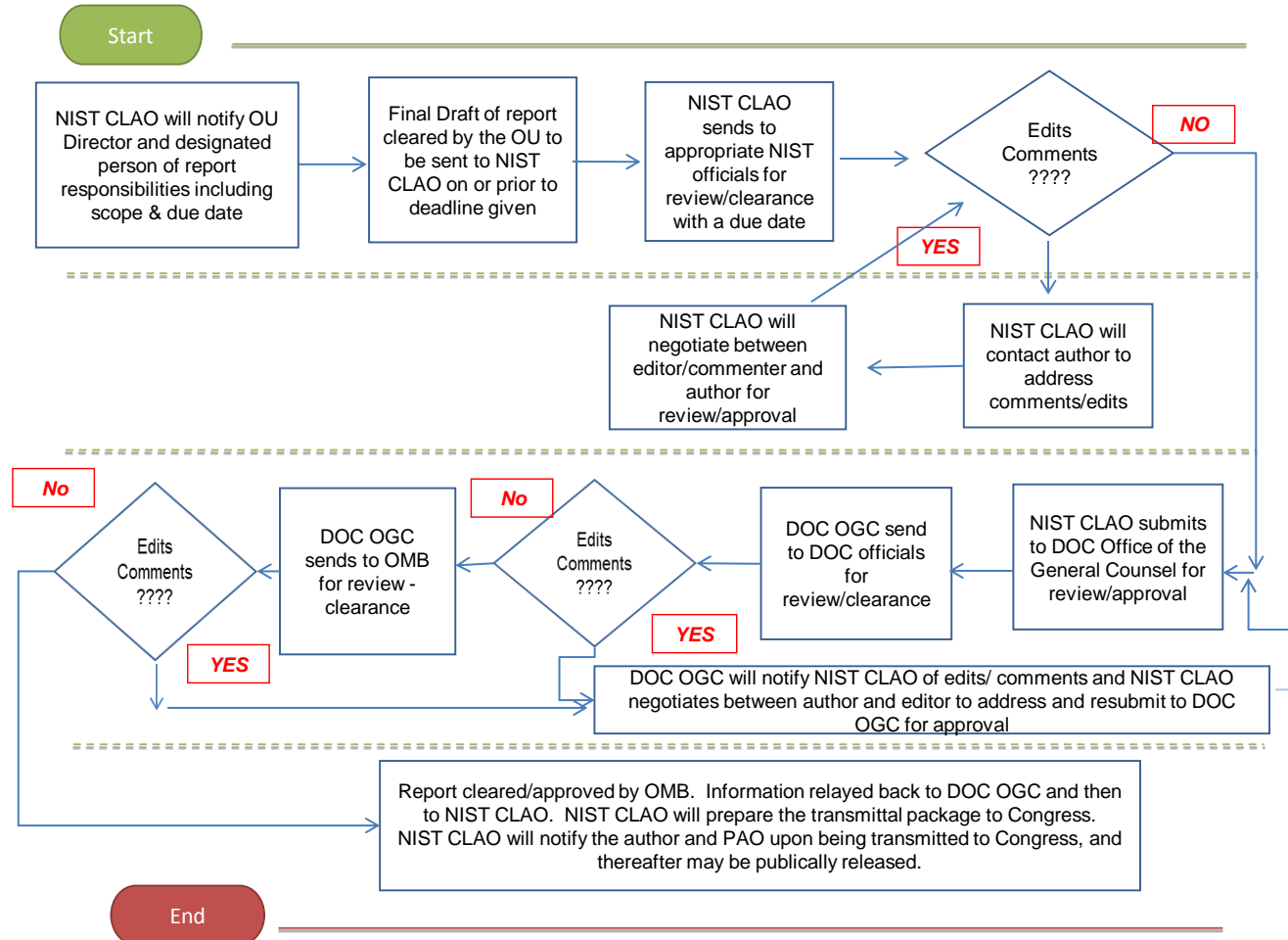
APPENDIX A

PROCESS FLOW DIAGRAM

General Process Flow in relation to:

Reports to Congress required under an Authorization law

as of 12/2/2014



APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/4/2012	Kandy Hauk	First Draft
Ver .01	9/5/2013	Dan Cipra	Formatting changes only
Ver .02	8/29/2014	Kandy Hauk	Edited
Ver .03	11/19/2014	Dan Cipra	Formatting changes only

Drafting and Clearance Procedures for Reports to Congress - Appropriations

NIST PR 1031.01
Effective Date: 7/30/2015

PURPOSE

This directive contains the National Institute of Standards and Technology's (NIST's) drafting and clearance procedures for reports to Congress that are required under an appropriations statute.

APPLICABILITY

The directive is applicable to all reports to Congress produced by NIST as required under an appropriations statute.

REFERENCES

- [Office of Management and Budget Circular No A-19](#)
- [Department of Commerce Organization Order DOO-10-6](#)
- [O 1030.00 Contacts with Congress and others 6/25/2014](#)

BACKGROUND

Appropriations statutes sometimes require NIST to submit reports to Congress to address specific issues. The NIST Budget Division (BD) in concert with Congressional and Legislative Affairs Office (CLAO) manages the required clearance process at NIST, the Department of Commerce (DoC), and the Office of Management and Budget (OMB) prior to any report being submitted to Congress.

All reports to Congress must be cleared by appropriate NIST officials, the DoC Office of Budget, OMB, and other agencies (if applicable). Once cleared, the DoC Office of Budget transmits the final report to the appropriate Congressional committees/subcommittees.

RESPONSIBILITIES

The Director of CLAO (or designee)

- Initially distributes congressional reporting requirements to the appropriate Organizational Unit (OU) Director and program within NIST containing the

responsibilities related to the report, including due dates for completion and submission of the report to CLAO.

The Director of the NIST Budget Division (or designee)

- Notifies the appropriate Budget Analyst within the BD to begin formal clearance process after receipt of the initial draft from CLAO.
- Manages the clearance process for sign-off of the final draft reports to Congress within NIST once the report has been initially vetted in draft by CLAO and forwarded to the BD.

Organizational Unit (OU) Director

- Assigns the appropriate OU Program Director (or designee) to draft the report and provides an OU internal due date.
- Reviews, edits, approves and sends the draft report to the CLAO.

PROCEDURES

1. The Director of CLAO (or designee) will send by email the specific congressional reporting requirement to the appropriate OU Director (or designee) notifying that person of his/her responsibilities which include: drafting the report, understanding its scope and providing the date the draft report is due back to CLAO.
2. The OU Director (or designee) assigns drafting of the report to the appropriate OU employee.
3. The OU-designated employee drafts the report and clears it through the OU before sending it back to CLAO within the established timeframe. The report must be forwarded to CLAO and received by the BD no less than 60 calendar days before the report is due to the requesting congressional committee. See item number four below.
4. The timeline is as follows: after the CLAO receives the initial draft report from the OU, the BD is sent the final draft *no less than 60 calendar days before the report is due to the congressional committee*. The responsible BD Analyst then routes the final draft report to the appropriate NIST officials using the official clearance sheet. Under no circumstances is there to be a waiver of NIST clearances and formal transmittal memos unless the BD is notified in writing of such a change by DoC. The deadline for the circulating clearance document to be returned to the BD is a maximum of 10 calendar days. This will allow the report to be forwarded to DoC in a manner that accommodates DoC's need for 50 calendar days to clear the document through DoC and OMB. Clearances of the following NIST officials are generally required: the Budget Officer, the Director of CLAO, the Chief Financial Officer, the appropriate Associate Director, the Chief of Staff, the Chief Counsel for NIST, and the Director of NIST.

5. After all appropriate NIST officials clear the initial draft report, the BD sends the draft report to the DoC Office of Budget for final routing clearance. If comments/edits are received, the BD coordinates the response with the author of the report and works to resolve any issues. After adjudicating all comments received, the BD submits the report to the DoC Office of Budget. After approving the report, the DoC Office of Budget sends it to OMB for the next level of required clearance.
6. OMB sends any comments/edits to the DoC Office of Budget, which in turn contacts the BD to coordinate a response. The BD contacts the author of the report to discuss the edits/comments received. After edits/revisions are made, and depending on the significance of such edits/revisions, the BD determines whether the revised sections of the report need to be re-cleared within NIST. The BD then resubmits the report back to the DoC Office of Budget. After the revised report is re-cleared by the DoC Office of Budget, that office sends the report to OMB for final review and clearance. When OMB approves the report, the DoC Office of Budget prepares the final transmittal package and sends it to the appropriate committees/subcommittees.
7. Once the DoC Office of Budget confirms that it has transmitted the report to Congress, the NIST BD will inform CLAO and the appropriate NIST OU of the completion of the congressionally mandated requirement.

DIRECTIVE OWNER

161 – Budget Division

APPENDICES

Appendix A: Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/4/2012	Kandy Hauk	First Draft
Rev. .01	9/5/2013	Dan Cipra	Formatting changes only
Rev. .02	1/31/2014	Kandy Hauk	Edited
Rev. .03	2/20/2015	Kim Carpentier	Edited
Rev. .04	3/25/2015	Melissa Lieberman	Edited
Rev. .05	4/8/2015	Kandy Hauk	Edited
Rev. .06	4/15/2015	Diane Holland	Edited
Rev. .07	4/16/2015	Dan Cipra	Formatting changes only
Rev. .08	4/30/2015	Francisco Balicao	Edited
Rev. .09	5/6/2015	Dan Cipra	Updates sent by budget div incorporated.

Public Communications

NIST O 1074.00
Effective Date: 4/30/2008

PURPOSE

This directive states the requirements for public communications for the National Institute of Standards and Technology (NIST).

APPLICABILITY

This directive applies to NIST Employees and Associates to the extent allowed by law and the terms of the Associates agreement.

LEGAL AUTHORITY AND REFERENCES

- [Department of Commerce Public Communications DAO 219-1](#)

REQUIREMENTS

- The DOC Public Communications Policy explicitly allows scientists and engineers to discuss basic or applied research results without prior approval from NIST's Public Affairs Office.
- Media interviews or other public statements involving policy, budget, or management require approval by NIST and DOC Public Affairs offices. News releases and news conferences also require approval. Contact your [Public Affairs Office contact](#) for guidance.

DIRECTIVE OWNER (DO)

107 – Public and Business Affairs Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/15/2013	Gail Porter	Initial Draft
Rev. .01	4/18/2016	Dan Cipra	Formatting updates only.

Conferences and Meetings

NIST O 1075.00
Effective Date: 2/22/2013

PURPOSE

This directive states the requirements, responsibilities, and procedures to be followed in the conduct of conferences sponsored, co-sponsored, or hosted by the National Institute of Standards and Technology (NIST).

APPLICABILITY

The following requirements are applicable to all NIST employees at all NIST facilities. This directive does not apply to Federal Advisory Committee meetings.

LEGAL AUTHORITY AND REFERENCES

- 15 U.S.C. 272a(3), 273, 275a and 278b
- Office of Legal Counsel - *Use of Appropriated Funds to Provide Light Refreshments to Non-Federal Participants at EPA Conferences* (April 5, 2007)
- Office of Legal Counsel- *Applicability of the Miscellaneous Receipts Act to Contractors Receiving Personal Convenience Fees from Attendees at an Agency-Sponsored Conference* (November 22, 2006)

DEFINITIONS

Conference - Any form of meeting, workshop, seminar, symposium, or training session. Federal Advisory Committee meetings are not conferences. This directive does not cover meetings or training for NIST staff only.

Hosted Conferences

- a. Conferences in which NIST acts solely as host (provides the facilities) but does not have lead involvement in the program. Examples of hosted conferences include Department of Defense meetings held at NIST, Department of Commerce (DoC) meetings held at NIST, and training courses for non-NIST employees.
- b. Conferences held at NIST must relate to some aspect of NIST's expertise or interests and must have a NIST employee act as liaison between the sponsoring organization and NIST.

No-cost contract

A no-cost contract is a formal arrangement between a government entity and a vendor under which the government makes no monetary payment for the vendor's performance. B-302811, July 12, 2004. "Under a typical no-cost contract, a vendor provides a service that [an] agency would otherwise perform, but instead of receiving compensation from the agency, the vendor charges and retains fees assessed against third parties for its services." B-300248, Jan. 15, 2004.

Sponsored or Co-Sponsored Conferences

- a. Conferences in which NIST acts as host (either offsite or when NIST provides the facilities) and NIST staff are heavily involved in planning, meeting content, and format. Usually, these are committee meetings of technical societies.
- b. Small technical training courses or seminars sponsored by NIST (e.g., the Precision Measurement Seminars) intended primarily for technical peers outside NIST. This excludes training courses organized by the NIST Office of Workforce Management Division intended primarily for NIST employees.
- c. If a decision is made to provide financial sponsorship for a conference through a grant, the Conference Program staff will provide guidance as needed and work with the programmatic representative.

REQUIREMENTS

- The planning of a NIST conference requires the active participation of a NIST organizational unit. A NIST programmatic division chief or a programmatic staff member appointed by the operating unit director must be involved in defining the scope and coverage of the specific conference. Such participation is necessary to ensure that NIST has a voice both in the programmatic aspects and the logistics of the conference. For a conference to be held at NIST, whether sponsored by NIST, co-sponsored by NIST or hosted by NIST, the topics discussed must align with NIST's mission.
 - a. For NIST sponsored conferences (either offsite or when NIST provides the facilities) the entire agenda and all logistics are developed by the NIST organizers.
 - b. For NIST co-sponsored conferences, the development of the agenda and logistics is shared with the co-sponsors.
 - c. For NIST hosted meetings, the agenda is developed by an outside organization; however, a representative of a NIST organizational unit must ensure that the topic being discussed aligns with NIST's mission.
- NIST collects and retains registration fees pursuant to 15 U.S.C. 275a and 15 U.S.C. 278b (NIST's Working Capital Fund authority).

- NIST conferences may be co-sponsored with other federal agencies, academic institutions, professional societies/associations, or private industry. NIST may sponsor or co-sponsor conferences provided that all of the following criteria are satisfied:
 - a. The conference is not budgeted to make a profit for the organizers. (See Approval Authorities and Budget Approval sections below.)
 - b. The conference is not used for commercial purposes by the co-sponsor
 - c. Every effort must be made to minimize conference costs including administrative costs, registration fees, and attendees' travel costs
 - d. Every effort must be made to maximize the use of government-owned or government-provided conference facilities
 - e. The cost of the selected conference lodging is within the per diem rate
- The NIST conference organizer should initiate the planning process, a minimum of three months in advance of the conference. In special cases, Public Affairs Office (PAO) will attempt to support conferences with less than three months' notice, but support cannot be guaranteed.
- If the conference involves food or beverages, NIST will use a contractor to help administer the conference. In most cases, PAO's Conference Program Group will be the Contracting Officer's Representative (COR) for the contract and, as such, will serve as the liaison with the contractor.
- For guidance and policies regarding publications or conference proceedings, refer to the [Editorial Review Board](#) (ERB).

APPROVAL AUTHORITIES

- Sponsored or Co-Sponsored Conferences

The NIST organizational unit planning the conference must complete Form NIST 1176, NIST Sponsored or Co-sponsored Meeting Approval, which is available via e-approval, and submit through their organizational unit (OU Director or designee) to the Conference Program Director (PAO) as soon as a conference is conceived, even if it is two years in advance. Templates for approval memos are available from the Conference Program staff.

- a. NIST expenses of \$20,000 or more, where NIST is a sole or co-sponsor, must be reported to the Department of Commerce and be approved by the NIST Chief Financial Officer (CFO).
- b. NIST expenses of \$75,000 or more, where NIST is a sole or co-sponsor, must be reported to the Department of Commerce and be approved by the NIST CFO and

the relevant NIST Associate Director, NIST Chief of Staff, Deputy Under Secretary of Commerce and Assistant Secretary of Commerce for Administration.

- c. NIST expenses of \$100,000 or more, where NIST is a sole or co-sponsor, must be reported to the Department of Commerce and be approved by all those listed in paragraph b. above and the Deputy Secretary of Commerce.
 - d. NIST expenses of \$500,000 or more, where NIST is a sole or co-sponsor, must be reported to the Department of Commerce and approved by all those listed in paragraphs b. and c. above and the Secretary of Commerce.
- Hosted Conferences

The outside organization must complete [Form NIST-1176A, NIST Meeting Approval - Non-NIST Sponsored Meetings](#). The signers of Form NIST-1176A are the person outside NIST who is responsible for the meeting (“conference organizer”); the NIST Programmatic Division Chief or a programmatic staff member appointed by the operating unit director, the Conference Program Director (PAO), and the NIST Chief of Staff.

BUDGET APPROVAL PROCESS

All conferences planned and executed by NIST, either sponsored or co-sponsored, onsite or offsite, must meet the follow requirements:

- a. A separate detailed budget for each event is developed by PAO. The budget must include the recovery of all costs, including PAO-incurred costs, and is developed with organizational unit representative input, approved through the Administrative Officer for PAO and the Conference Program Group Leader, PAO. A copy of each budget is forwarded to the Receivables Group of the Finance Division. A separate PAO project-task is established for each conference to collect fees and costs associated with each conference. Budgets for conferences should be developed at an early planning meeting by the Conference Program Group in consultation with the NIST organizational unit representative.
- b. Approval of a separate budget is required for each fee-supported conference even though it may be a continuation or periodic reconvening of a previously approved conference.
- c. For meetings where NIST is not collecting registration fees (co-sponsored or hosted), the PAO budget includes only the portion of the conference budget costs that will be incurred by NIST.
- d. The budget for each conference must be planned to recover all direct expenses of the conference. Budgets will not be designed to make a profit for any reason, including the start-up of a future conference.
- e. After the final budget has been approved, charging must be consistent with the approved budget.

- f. A budget may be revised to add, change, or delete line items or amounts. Revised budgets must also break even and must go through the same approval process as the original budget. Revisions affecting the registration fees must be approved before publishing the fees. No revisions that affect the registration fees will be approved after fees for the conference are published.
- g. While conference budgets are planned to break even, conference attendance fluctuations result in profits and losses in conference project-tasks. All profits and losses will remain in the individual PAO conference project-task. At the end of each fiscal year, all profits and losses within this series are netted against the profits and losses from all other reimbursable activities.
- h. If conference pre-registration falls well below the attendance level upon which the budget had been based, PAO (in consultation with the NIST sponsor) will decide if the conference will be canceled. In the event of cancelation, all registration fees collected will be returned to registrants.

When a meeting to be planned and executed by NIST requires catering or other special services, a contractor may be required. NIST programmatic representatives must consult with the Conference Program Office, PAO, about whether a contractor is required for a given event. Depending on the services required, either a “no cost” contract or contract that requires payment to the vendor may be appropriate.

- Conferences Planned and Executed by NIST and a PAO no-cost contractor
 - a. A separate budget for each event is developed by PAO in coordination with a no-cost contractor, based on pre-established costs that have been negotiated between NIST and the no-cost contractor. To ensure proper handling of federal expenses, the NIST Budget Division reviews and approves conference expenses paid with NIST appropriated funds.
 - b. A Performance Work Statement (PWS) will be generated in PAO to establish a task order with the no-cost contractor.
 - c. Registration fees collected by the no-cost contractor must be clearly defined and approved by NIST prior to the awarding of the task order. The no-cost contractor will use the conference attendee registration fees it collects to pay for all items required for the conference. A detailed accounting of collections and disbursements will be required for each conference including NIST charges. To the extent the contractor will be collecting a fee for refreshments or other personal convenience items (“personal convenience fee”), NIST may ensure that the contractor’s arrangements are not lavish; however, it cannot otherwise direct the arrangements.
 - d. As directed by NIST, the no-cost contractor will furnish the necessary personnel, material, equipment, and services and facilities to perform the PWS. PAO will bill the no-cost contractor for NIST costs.

- e. A budget may be revised to add, change, or delete line items or amounts. If so, the PWS must be amended to reflect the revision.
- f. If conference pre-registration falls well below the attendance level upon which the budget had been based, PAO (in consultation with the NIST sponsor or NIST organizational unit representative) will decide if the conference will be canceled. If the conference is canceled, all registration fees collected will be returned and the task order will be canceled at no cost to the government.
- Conferences Planned and Executed by NIST and a paid contractor
 - a. A paid contractor may be appropriate for meetings that require technical services such as analytical support, technology monitoring and analysis, event logistics, workshop development, report development, and expert planning advice and guidance. Each task order will have a Contracting Officer's Representative from the NIST programmatic division.
 - b. The contractor may collect the registration fees for the conference directly from the attendees of the conference based on the requirements in the task order. The fees collected by the contractor must be clearly defined and approved by NIST PAO (with the exception of any personal convenience fee) prior to the awarding of the task order and should cover all items required for the conference. A detailed accounting of collections and disbursements will be required for each conference. As directed by NIST, the contractor will furnish the necessary personnel, material, equipment, and services and facilities to perform the PWS. PAO will bill the contractor for NIST charges.
 - c. A budget may be revised to add, change, or delete line items or amounts. If so, the PWS must be amended to reflect the revision.
 - d. If the conference is canceled, all registration fees collected will be returned to registrants.
- Conference Sponsorships through Grants and Contracts

If a decision is made to provide financial sponsorship for a conference through a purchase order, grant or interagency agreement, then NIST programmatic staff will work with appropriate staff from either the NIST Acquisition Management Division (AMD) or the Grants and Agreements Management Division (GAMD) to execute the financial transaction. AMD and GAMD will require an approved Form NIST-1176 as well as documentation of additional Departmental approvals (if required) prior to initiating the financial transaction. Conference Program staff will provide guidance as needed and work with the programmatic representative.

CONFERENCE FINANCING

- Registration fees are used to reimburse NIST and its contractors for the costs of providing services to the conference participants and are determined by developing the

conference budget. For sponsored or co-sponsored meetings, registration fees can be reduced by contributions/sponsorships from outside sources or the sponsoring organization. The following are cost components of the registration fee for conferences *not* involving food or beverages:

- a. The PAO fee is established to cover the direct costs of the services provided by the Conference Program Group staff, PAO
 - b. In addition to PAO fees, NIST is permitted to pay for the following items that may be included in a conference budget:
 - Printing and duplicating, including printing of proceedings;
 - Speaker travel;
 - Communications such as flyers, brochures, etc.;
 - Rental of equipment such as AV equipment or poster display boards, etc.;
 - Rental of non-NIST conference rooms;
 - Services of registration, recording stenographers, foreign language translators, or other specialized individuals; and
 - Labor directly associated with the running of the conference
 - c. Occasionally an organizational unit will want to publicize a conference in the very formative planning stage or do an advance mailing to estimate the level of interest and/or call for papers. [Form NIST-1176](#) must be completed and PAO contacted to make printing and mailing arrangements before any “Save the Date” mailings or e-mails are issued. The conference budget should be approved six weeks before the preliminary mailing. Should sufficient interest not materialize to warrant holding a conference, costs incurred by PAO for this preliminary mailing will be transferred to the organizational unit.
- Serving refreshments during conference breaks, holding luncheon meetings, receptions, and banquets is frequently desired. If deemed necessary, NIST must use a contractor with a no-cost line item for personal convenience items to facilitate such a conference. (See Budget Approval section above.) As of April 2, 2008, appropriated funds (which include registration fees collected by NIST) may not be used to purchase refreshments for conferences, absent specific statutory authority. NIST ensures that registration fees collected for food items fall within the Federal per diem allowance guidelines whenever possible.
 - Non-Fee Registration
 - a. The Conference Program Group staff, PAO also provides some services for smaller meetings or conferences that do not require a registration fee. For meetings of more than 35 people but fewer than 100 people, where the NIST programmatic unit conducts its own registration, the Conference Program Group staff will handle the basic logistics for the meeting at no charge to the NIST organizing or sponsoring unit for a minimal fee. This logistics include providing name badges and

- coordinating security needs. Attendees not paying a registration fee are responsible for buying their own coffee or other refreshments and lunches when onsite.
- b. For meetings where the NIST programmatic unit does not wish to charge a registration fee, but the attendance is estimated to be greater than 100 people, the sponsoring division must electronically register the attendees through the Conference Program. The sponsoring organization should complete [Form NIST-461, Interdivision Work Order](#), to transfer the applicable service fees to the Conferences Program Group, PAO.
- Financial Responsibilities (for conferences not involving food or beverages)
 - a. Conference finances are handled by PAO through the NIST accounting system or by a co-sponsor. NIST may not handle conference funds on behalf of a co-sponsor.
 - b. Registration fees collected by NIST are collected by the Receivables Group in the Finance Division. The Finance Division then provides PAO with attendee registration information.
 - c. Cost accounting for some conferences may span two or more fiscal years. PAO will inform the Finance Division of the requirements for either:
 - Deferring income collected in one fiscal year to cover costs which will not accrue until the following fiscal year, or
 - Submitting work-in-process estimates to cover costs incurred prior to the receipt of income
 - Collection of Registration Fees (for conferences not involving food or beverages)
 - a. Registration Fees Collected by NIST
 - Registration fees are established through development of the conference budget, using information provided by the NIST conference organizer to the Conference Program Group staff, PAO, approved by the Budget Division, and collected by the Finance Division.
 - The conference registration fee will be set to cover costs of the conference for which the budget is being prepared only. Registration fees will not recover losses for previous conferences, nor collect income for expenses associated with future conferences. However, the cost of conference steering committee meetings to plan a conference may be included in that conference's budget.
 - Registration fees may deviate among conference participants only as follows: early, late, student, and partial (when appropriate, e.g., one-day, tutorial, etc.) and only to the extent that the deviation represents a legitimate cost difference to the government.
 - Registration fees may not be set to recover all costs from one group of participants while not charging another group of participants (excluding speakers).

- Payment of registration fees will be made to the Finance Division via credit card. Registration must include a list of conference participants whose registration fees are covered by the payment.
- Advance payment of registration fees must be strongly encouraged in all conference brochures.

RESPONSIBILITIES

Sponsored or Co-Sponsored Conferences

NIST Chair (for that conference)

- Assumes responsibility for agendas
- Assist with conference support as appropriate
- Initiates the request to sponsor or co-sponsor a conference and receives approval from the division chief or above
- Accepts ultimate responsibility for the technical content of the program
- Works with PAO to monitor meeting planning and execution
- Plays a major role in planning and approving program content and format, selection of speakers, planning proceedings, and scheduling the program
- Provides a website for the meeting and coordinates with PAO on the format and content
- Provides and coordinates with PAO appropriate materials needed to publish conference announcements, programs, and abstracts
- Consults with the Electronic Information and Publications Program, Information Services Office, to ensure that plans for NIST to publish proceedings are feasible
- Assists in the actual conduct of the conference by providing session monitors, registrars, and other staff as needed
- Works with PAO regarding publicity, including news releases, press advisories, news conferences, and electronic conference announcements, as appropriate
- Identifies mailing and e-mail lists to reach targeted audience

When a conference is co-sponsored with one or more organizations, these responsibilities may be shared by the co-sponsors. A NIST representative serves as the primary liaison between the co-sponsors and the NIST Conference Program. If a conference is supported by a grant, consult Conference Programs for guidance.

The Conference Program Group, PAO

- Provides general assistance in advance planning of conferences. Assists NIST conference planners in using the DoC Conference Planning Checklist to ensure

compliance with DOC and NIST conference policies, that spending is appropriately controlled, and that proper controls are in place.

- Ensures that the promotion activities preceding meetings and the actual meetings run smoothly and professionally
- Provides the participants with conference services required at such meetings
- In most cases, acts as the COR on contracts needed for NIST meetings
- PAO maintains a contract with a no cost contractor

The Audio-Visual Services Group, PAO, (when requested)

- Provides audiovisual services and is responsible for the set up, operation and removal of and/or shutting down of equipment for meetings

Budget Division

- Reviews and approves or disapproves all NIST charges included in conference budgets.

Receivables Group, Finance Division

- Supports PAO in updating the conference database with registration and payment information
- Processes and collects registration fees in the NIST accounting system
- Provides refunds to conference attendees as requested by PAO
- Invoices for registration fees as requested by PAO

Acquisition Management Division

- Awards contracts for services needed to run conferences

Grants and Agreements Management Division

- Awards grants and cooperative agreements for conference related activities

Editorial Review Board (ERB)

- For further guidance on publishing conference proceedings see <http://www-i.nist.gov/admin/mo/adman/409.htm#4.09.07>

DIRECTIVE OWNER (DO)

107 – Public and Business Affairs Office

APPENDICES

A. NIST In-House Conference Services

B. Revision History

APPENDIX A

NIST In-House Conference Services

The services provided by the NIST Conference Program staff vary according to the type of meeting. The fee for these services is included in the conference budget and is determined by the range of services provided. These services may include:

- Develop a planning schedule
- Help reserve meeting room space
- Conduct site searches and selections for off-site meetings
- Review and approve all items to be expended by the conference and prepare a detailed budget
- Coordinate promotional materials to encourage attendance and attract media coverage
- Produce printed materials and arrange mailings
- Coordinate electronic publicity
- Coordinate with hotels for special arrangements
- Handle registration, provide confirmations, and mail receipts to attendees
- Provide name badges and participant lists
- Prepare handout materials
- Plan, but not pay for, food functions at NIST and off-site locations;
- Plan room arrangements, including audiovisual requirements and poster sessions
- Arrange tours and special events at NIST and off-site meetings
- Oversee conference displays (e.g., arrange for poster panels and moving services)
- Coordinate the production and placement of signs
- Handle last-minute photocopying needs
- Coordinate parking and security needs
- Process proceedings
- Monitor conference project-tasks
- Process and track work orders and purchase orders
- Survey conference attendees and prepare conference evaluation form results
- Provide a final expense and income report

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/15/2013	Kathy Kilmer	Initial Draft
Rev. .01	4/18/2016	Dan Cipra	Updated PAO and removed reference to admin manual subchapter.

Directives Management System

NIST P 1100.00
Effective Date: 10/25/2011

PURPOSE

To ensure the effective management and operation of NIST, it is essential to provide staff with accurate and authoritative information regarding the policies, requirements and procedures needed for the administration and operation of NIST programs and activities.

SCOPE

The provisions of this policy apply to all NIST federal employees and Associates to the extent allowed by law and the terms of the Associate's agreement. This policy establishes the environment for the NIST Directives Management System (DMS) which will replace the NIST Administrative Manual, as the primary communication system for NIST operations and administrative documents.

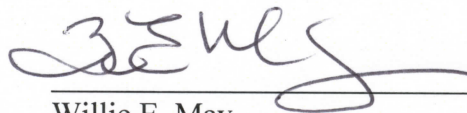
LEGAL AUTHORITY

- [The NIST Act, 15 United States Code §§ 271 et seq.](#)
- [Department of Commerce, Department Organization Order \(DOO\) 30-2A.](#)

POLICY

It shall be the policy of NIST to establish a system of directives to define, organize, and officially communicate policies, requirements, procedures, and guidance needed for the administration and operations of NIST programs and activities. The information in the DMS will be organized into separate categories (i.e., policy, requirements, procedures, guidance) with a common subject numbering system to enable personnel to efficiently find information.

The NIST Chief of Staff is responsible for developing the requirements for the DMS and for maintaining it as a viable resource for accomplishing the mission of NIST. NIST organizations are responsible for developing and maintaining directive content and for ensuring accurate, up-to-date, and readily available information for use by staff and others to carry out assigned duties.



Willie E. May
Director

7/24/15
Date

ORDER

NIST O 1110.00

Approved: 6/13/2014

Effective: 6/13/2014

DIRECTIVES MANAGEMENT SYSTEM



Directive Owner:
Management and Organization Office

Table of Contents

1. PURPOSE.....	1
2. APPLICABILITY	1
3. REFERENCE.....	1
4. DEFINITIONS.....	1
5. REQUIREMENTS	3
6. RESPONSIBILITIES AND AUTHORITIES.....	3
7. DIRECTIVE OWNER.....	5
8. APPENDICES.....	6
APPENDIX A – DIRECTIVES MANAGEMENT SYSTEM (DMS) DOCUMENT TEMPLATES.....	7
APPENDIX B - DIRECTIVES PROCESS FLOW FOR DIRECTIVES REVIEW BOARD (DRB) CLEARANCE	15
APPENDIX C SUBORDER PROCESS	21
APPENDIX D GUIDANCE PROCESS.....	22
APPENDIX E - DIRECTIVE NUMBERING.....	23
APPENDIX F - REVISION HISTORY	25

NIST Directives Management System

NIST O 1110.00
Effective Date: 6/13/2014

1. PURPOSE

This directive provides an overview of and defines the structure and requirements of the NIST Directives Management System (DMS) and assigns the authorities, roles and responsibilities. In addition, it establishes the overall directives numbering structure and provides templates for directives along with a process flow for directives. This directive replaces NIST N 250, DMS Implementation Plan in its entirety.

2. APPLICABILITY

This directive is applicable to all NIST employees who have responsibilities related to directives.

3. REFERENCE

The authorization for this directive is specified in [NIST Policy 250.01 Directives Management System](#) (approved 10/25/11)

4. DEFINITIONS

- 4.1. Approving Official – NIST Director, Associate Director or Chief Officer, or other person designated by the director, responsible for the approval of the directive.
- 4.2. Contact Person– The person designated by the Directive Owner (DO) as the point of contact for each directive.
- 4.3. Deployment Tools - A checklist, diagram, flowchart, IT application or other means used in a directive to assist the reader in understanding the subject matter.
- 4.4. Directive Owner (DO) – The management of the organization responsible for the document throughout the entire directives document lifecycle. The DO also will ensure the information set forth in the directive is communicated to their stakeholders as appropriate.
- 4.5. Directives Management System (DMS) - A system of formal written communications to define, organize and officially convey/transmit/communicate policies, requirements, responsibilities, procedures and guidance needed for the administration and operations of NIST programs and activities.
- 4.6. Directives Review Board (DRB) - A group of administrative and technical subject matter experts chartered by NIST leadership to provide vetting of NIST directives and advise the approving official on individual directives and to support implementation.

The DRB is chaired by the Assistant Chief of Staff and functions based on its charter. The [DRB Charter](#) contains a listing of members along with other important information.

The DRB does not approve directives; it is chartered to review the documents and to provide a recommendation(s) to the approving official.

- 4.7. Guidance – Non-mandatory, advisory information provided to support implementation of an Order, Suborder, Procedure or Notice. Examples may include best practices or lessons learned. Guidance will not be formally reviewed or approved by the DRB. The guidance template is located in Appendix A, and the process for guidance directives is located in Appendix D.
- 4.8. Legal Sufficiency –The document complies with current law, regulations, and policies.
- 4.9. NIST Administrative Committee – An officially chartered committee responsible for vetting and approving suborders that fall under their purview. No suborders may be published in the DMS without documented approval of the appropriate administrative committee. See [NIST O 205 Administrative Committees](#).
- 4.10. NIST Form 290 Directives Routing Sheet: - The form used to record information about each directive and serves as the workflow routing document for clearance and approval of each directive.
- 4.11. NIST Vetting Process – A process the DO and contact person perform for each directive including review by those representatives within the DO organization and other NIST organizations governed by the directive.
- 4.12. Notice – A temporary directive issued in response to any matter requiring prompt action. Notices are reviewed annually and automatically renewed unless rescinded by the DO.
- 4.13. Order – A directive that establishes authorities, requirements and assignment of responsibilities and addresses “what” needs to be done.
- 4.14. Policy – A directive that sets the expectations or helps to create the environment to be established by the NIST Director. A Policy is implemented through issuance of orders, procedures and other directives depending on what is required.
- 4.15. Procedure - A directive defining a specific series of actions, tasks or operations that must be executed in the same manner to always obtain consistent results. A Procedure prescribes “how” a particular policy or order is carried out.
- 4.16. Suborder – A directive that establishes authorities, technical requirements and assignment of responsibilities in a specific subject area under an order and focuses on the technical details of the program. Each suborder must be vetted and approved by the applicable NIST Administrative Committee. Suborders will normally be made available to the DRB for information purposes only. The suborder template is located in Appendix A, and the process for suborders is located in Appendix C.

5. REQUIREMENTS

- 5.1. This Order sets forth the DMS, the system through which NIST defines, organizes and officially communicates organizational directives needed to carry out the mission of NIST.
- 5.2. This Order sets forth the responsibilities and delegates the authority to create, execute, implement and maintain the directives comprising the DMS.
- 5.3. Directive content shall be written in active voice using plain English with minimal use of jargon. The information shall be intuitive, accurate and up-to-date. The NIST directive templates are found in Appendix A.
- 5.4. Through the DMS, NIST defines the structure needed for the administration and operation of NIST programs and activities. The [NIST DMS process flow](#) is found in Appendix B. The DMS Directive Numbering is found in Appendix E.
- 5.5. The DMS is made up of all NIST directives, including:
 - a. New need-based directives that NIST organizations identify
 - b. Directives migrated from the NIST Administrative Manual and other policy-related documents
- 5.6. Directives will be continuously monitored by the DO to ensure conformity to all new or revised legal authorities, references and administrative policies within a reasonable time period, not to exceed 24 months.

6. RESPONSIBILITIES AND AUTHORITIES

- 6.1. NIST Director
 - 6.1.1. Serves as final approval authority for all NIST directives. This authority may be delegated.
- 6.2. NIST Chief of Staff or Designee
 - 6.2.1. Serves as the liaison to the NIST Director for the DRB, and is hereby delegated authority from the NIST Director to implement DMS requirements.
 - 6.2.2. Maintains the DRB Charter and the membership roster. Serves as the chair of the DRB.
 - 6.2.3. Manages the DMS, the directive development process, and the disposition of DRB review comments.
- 6.3. NIST Associate Directors
 - 6.3.1. Serve as final approval authority (delegated from NIST Director) for all NIST Orders, Suborders, Procedures, and Notices in their respective areas of responsibility, may further delegate that approval authority to the appropriate OU Directors or designee.

- 6.3.2. Ensure all required directives in their areas of responsibility are developed using the process directed by the DMS.
- 6.3.3. Oversee implementation of all approved directives.
- 6.4. OU Director or Designee
 - 6.4.1. Develops a directives strategy to support their area.
 - 6.4.2. Assigns a Contact Person for each directive.
 - 6.4.3. Follows the DMS process while developing directives.
- 6.5. Directives Review Board
 - 6.5.1. Functions as the final recommendation authority for all directives.
 - 6.5.2. Reviews all directives and ensures that:
 - a. Each directive is written in active voice using plain language;
 - b. The content matter is presented in a manner that makes the material covered intuitive;
 - c. The information is accurate; and
 - d. The directive is kept up-to-date.
 - 6.5.3. Meets at the call of the DRB Chair to conduct necessary committee business.
 - 6.5.4. Works closely with M&O to ensure the directive review cycle is followed to keep the pipeline of documents at a manageable level.
- 6.6. NIST Administrative Committees
 - 6.6.1. As designated in their charters, these administrative committees may provide the authority for the DO to draft and publish sub-orders within the DMS.
 - 6.6.2. Ensure that the sub-orders are properly vetted.
- 6.7. Management and Organization Office (M&O)
 - 6.7.1. Functions as the secretariat for the DRB, responsible for scheduling meetings, managing the agenda and publishing minutes.
 - 6.7.2. Provides advice and consultation on the format, composition, and presentation of directives.
 - 6.7.3. Maintains the authoritative version of each directive and clearance sheet.
 - 6.7.4. Coordinates with the responsible DOs to ensure they are familiar with and maintain an acceptable review cycle for each directive.
 - 6.7.5. Publishes NIST directive content on the NIST internal website.
 - 6.7.6. Monitors the NIST internal website and ensures only approved directives are displayed.

- 6.7.7. Removes all unauthorized directives from the NIST internal website and notifies the DO and the DRB of the removal.
- 6.7.8. Manages the directives database and provides the DRB and DOs with status reports.
- 6.8. Directive Owner
 - 6.8.1. For each directive under their purview, works with the organization's Contact Person, who functions as directive author and point-of-contact for the NIST vetting process.
 - 6.8.2. Performs regular reviews of all directives in their purview in accordance with the DMS process.
 - 6.8.3. Notifies M&O when a directive changes or any link in any directive is changed.
- 6.9. Contact Person
 - 6.9.1. Coordinates and/or reviews content prior to vetting to ensure consistency with other directives.
 - 6.9.2. Collaborates with their OU Leadership to ensure the directives under their control are properly vetted before submitting to the DRB.
 - 6.9.3. Performs the NIST vetting process for each directive, ensuring that the directive is vetted through organizations with responsibilities set forth in the directive, as well as internal stakeholders, focusing on content, usability and readability.
 - 6.9.4. Works closely with all pertinent NIST and DoC organizations as necessary during the directive draft/review stage.
 - 6.9.5. Completes the NIST Form 290 and follows the DRB submission process.
 - 6.9.6. Revises and updates directive content as required and according to the DMS process.
 - 6.9.7. Disseminates the directive as necessary.
- 6.10. Office of the Chief Counsel for NIST
 - 6.10.1. Reviews and clears all directives for legal sufficiency and accuracy.
 - 6.10.2. Vets directives with all appropriate Office of General Counsel offices.
- 6.11. Public and Business Affairs
 - 6.11.1. Provides guidelines for NIST internal website publishing and other content that will affect the DMS and publication of directives.

7. DIRECTIVE OWNER

101 - Management and Organization Office (M&O)

8. APPENDICES

- A. Directives Management System (DMS) Document Templates
- B. Directives Process Flow for Directives Review Board (DRB) Clearance
- C. Suborder Process
- D. Guidance Process
- E. Directive Numbering
- F. Revision History

APPENDIX A

APPENDIX A – DIRECTIVES MANAGEMENT SYSTEM (DMS) DOCUMENT TEMPLATES

The DMS document templates provide the current format and required information for all directives. The purpose of the templates is to provide a standard format for each type of NIST DMS document. All sections are mandatory unless marked optional. The Directive Owner (DO) may add sections or other elements, such as a table of contents that are not currently included in the template. If there are questions or issues concerning any of these templates, contact the Management and Organization Office (M&O) for assistance.

General Template information

- Cover page - Optional
- Table of contents - Optional
- Each document drafted contains a header and footer
 - The header, located only on the first page of the directive, contains the NIST logo, the directive name and number, and the effective date
 - The footer, located on every page except the cover page, includes the directive number and version, the statement “(Uncontrolled copy in print)” and the page number
- The font is Times New Roman 12
- The line spacing is 1.15
- The paragraph spacing is 6pt and 12pt between sections
- The sections and subsections may be numbered or bulleted and can contain multi-level numbering also referred to as coordinates.

Deployment tools

The use of deployment tools in a directive often assists in the understanding of the subject matter. Types of deployment tools include checklists, IT applications, diagrams, and flowcharts. These tools should be made accessible through the use of links or in appendices.

Appendices

Appendices should be used as needed in directives; they should appear in order as they are referred to in the text of the document.

TEMPLATE

This Cover Page is to be used whenever the Directive includes a table of contents.

Directive Type

NIST X ####.##

Approved: MM-DD-YYYY

Effective: MM-DD-YYYY

SAMPLE COVER PAGE (optional)



Directive Owner:
Name of Organization

Policy Title (Template)

NIST P XXXX.XX
Effective Date: MM/DD/YYYY

PURPOSE

Define the program or subject matter and its goals/objectives. Goals should be stated in simple, straightforward language that describes the results to be achieved by issuance of the directive.

SCOPE

Define to whom the directive applies to e.g., NIST employees.

LEGAL AUTHORITY AND REFERENCES

- Cite all applicable laws, regulations, government-wide directives or policies, Department of Commerce policies, and directives in bulleted format.

POLICY

Sets the expectations of the authority setting the policy or helps to create the environment that is desired to be established. Ultimately guides decisions in order to achieve a desired outcome.

Include a paragraph that delegates or identifies the NIST official that will be responsible for ensuring this policy is implemented and maintained.

_____ APPROVING OFFICIAL TITLE	_____ DATE
--------------------------------------	---------------

Order Title (Template)

NIST O XXXX.XX
Effective Date: MM/DD/YYYY

PURPOSE

Define the program or subject matter and its goals/objectives. Goals should be stated in simple, straightforward language that describes the results to be achieved by issuance of the directive.

APPLICABILITY

Define to whom the directive applies to e.g., NIST employees.

REFERENCES

- Cite all applicable laws, regulations, government-wide directives or policies, Department of Commerce policies, and directives in bulleted format.

REQUIREMENTS

List each requirement here. This is “what” needs to be done.

DEFINITIONS (Optional)

Term – define the term here

RESPONSIBILITIES

List the organization and title of the applicable NIST official(s) here and a bulleted list of responsibilities for each

Office of the Director

- List each Responsibility here

DIRECTIVE OWNER

Organization Number - Organization Name

APPENDICES

- A. List each appendix here

Suborder Title (Template)

NIST S XXXX.XX

Issue Date: XX/XX/XXXX

Effective Date: MM/DD/YYYY

PURPOSE

Define the program or subject matter and its goals/objectives. Goals should be stated in simple, straightforward language that describes the results to be achieved by issuance of the directive.

APPLICABILITY

Define to whom the directive applies to e.g., NIST employees.

REFERENCES

- Cite all applicable laws, regulations, government-wide directives or policies, Department of Commerce policies, and directives in bulleted format. At a minimum, the policy and/or order related to the suborder must be listed.

DEFINITIONS and or ACRONYMS (Optional)

Term – define the term here

REQUIREMENTS

- List each requirement here. This is “what” needs to be done.

ROLES AND RESPONSIBILITIES (Optional)

List the organization and title of the NIST official(s) here and a bulleted list of roles and responsibilities for each

Office of the Director

- List each Responsibility here

PROCEDURES CHECKLISTS/GUIDELINES (Optional)

Please list suborder-specific procedures here.

DIRECTIVE OWNER

Organization Number - Organization Name

APPENDICES

List each appendix here

Procedure Title (Template)

NIST PR XXXX.XX

Effective Date: MM/DD/YYYY

PURPOSE

This document establishes procedures for the program, including responsibilities, and details outlining the specifics of the program.

APPLICABILITY

Define to whom the directive applies to e.g., NIST employees.

REFERENCES

- List references including government-wide and related NIST directives

DEFINITIONS (Optional)

Term - definition

RESPONSIBILITIES

List the organization and title of the NIST Official(s) here and a bulleted list of roles and responsibilities for each

Office of the Director

- List each Responsibility here

PROCEDURES/CHECKLISTS/GUIDELINES

Insert the deployment tool to be used; this section is tailorable and may include links to authoritative information and in some cases may include substance.

DIRECTIVE OWNER

Organization Number - Organization Name

APPENDICES

- A. List each appendix here

Guidance Title (Template)

NIST G XXXX.XX

Effective Date: MM/DD/YYYY

PURPOSE

This document establishes guidance for a program or administrative process. Because compliance with information is not mandatory, the directive owner will provide information, not requirements or responsibilities. This guidance may take the form of best practices, lessons learned and other documentation helpful to the audience.

APPLICABILITY

Define to whom the directive applies to e.g., NIST employees.

REFERENCES

- List references including government-wide and related NIST directives

DEFINITIONS (Optional)

Term - definition

GUIDANCE

Insert the sections based on the needs of the document; this section is tailorable and should use links to authoritative information

DIRECTIVE OWNER

Organization Number - Organization Name

APPENDICES

- A. List each appendix here

Notice Title (Template)

NIST N XXXX.XX
Effective Date: MM/DD/YYYY

PURPOSE

Define the program or subject matter and its goals/objectives. A notice can be issued in place of a Policy, Order, Procedure or Guidance so the template will be tailorable. Goals should be stated in simple, language that describes the results to be achieved by issuance of the directive.

APPLICABILITY

Define to whom the directive applies to e.g., NIST employees.

REFERENCES

- Cite all applicable laws, regulations, government-wide directives or policies, Department of Commerce policies, and directives in bulleted format.

REQUIREMENTS (if related to an order or suborder)

- List each requirement here. This is “what” needs to be done.

DEFINITIONS (Optional)

Term – define the term here

RESPONSIBILITIES (if an order or procedure)

List the organization and title of the NIST Official(s) here and a bulleted list of roles and responsibilities for each

Office of the Director

- List each Responsibility here

PROCEDURES (if related to a suborder or procedure)

Insert the deployment tool to be used; this section is tailorable and may include links to authoritative information and in some cases may include substance.

DIRECTIVE OWNER

Organization Number - Organization Name

APPENDICES

A. List each appendix here

APPENDIX B

APPENDIX B - DIRECTIVES PROCESS FLOW FOR DIRECTIVES REVIEW BOARD (DRB) CLEARANCE

The directives process contains separate process flows, one for new directives and the other for updating existing directives:

New Directive – This process is used for a new directive, whether a conversion from an existing NIST Administrative Manual subchapter or a directive created by the DO for the first time.

Update Existing Directive – This process is used only for an existing directive and may occur any time after initial publication. This would also apply to an existing directive being updated to a different type of directive.

Suborders and Guidance directives do not require DRB clearance. These directives will not be formally reviewed or considered by the DRB; informational copies will be provided to all DRB members by the Management and Organization Office (M&O).

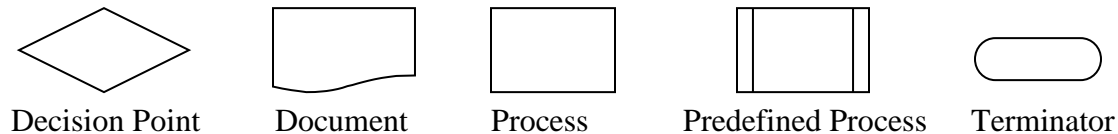
The new and existing directive processes contain four parts:

1. **Initiation** – The DO identifies their document strategy, including the creation/review of a draft/published directive including proper formatting and numbering of the directive within the DMS.
2. **Vetting** – The DO conducts internal and stakeholder vetting of the draft document. The DO should, at a minimum, route the document through those Organizational Units (OUs)/Offices that are mentioned in the directive and that have a role or responsibility. This part may include legal review by the NIST Office of Chief Counsel (OCC) or the appropriate DoC Office of General Counsel for review. The DO is ultimately responsible for the directive and must ensure the vetting is complete. The last step is the DO certification of the directive on the NIST Form 290 and transmittal to M&O.
3. **Clearance and Approval** – M&O first determines the type of DRB review, electronic or formal DRB Meeting. As the DRB secretariat M&O prepares and routes the package to the DRB members and representatives. During this cycle the DO will work directly with each DRB member that comments on the document, creating a collaborative environment that concludes with the DRB voting to make a recommendation to the approving official. The signature of the approving official on the NIST Form 290 marks the conclusion of this part.
4. **Dissemination** - M&O publishes the interim directive on the NIST internal web site, updates the DMS database. After a 45 business day period for OCC comment, the directive will go final and M&O schedules the directive for the next review cycle. If there is feedback, OCC will provide comments to the DO and M&O, the approving

APPENDIX B (continued)

official will have the final determination. The DO then disseminates the directive according to their communication strategy.

In order to provide a clear picture, included are a numbered listing and a visual process flow representation using standard symbols as follows:



New Directive Process Flow (does not apply to suborders and guidance)

(each numbered item below corresponds to a specific block on the diagram):

1. Directive Owner (DO) contacts M&O to create a new directive.
2. M&O and DO meet to discuss the new directive and the DO strategy.
3. DO drafts directive and sends to M&O.
4. M&O reviews the draft directive and ensures proper format.
5. Directive is returned to the DO for NIST vetting.
6. DO vets new directive with their NIST stakeholders/customers (legal as required).
7. DO updates the draft and completes NIST Form 290.
8. DO sends the draft directive package to M&O.
9. M&O determines the DRB review type (Electronic or Formal DRB Meeting).
10. M&O prepares/sends the Package to the DRB, including the draft directive and a comment sheet for their review and comments.
11. DRB members return comment sheet back to M&O, who consolidates the comments and sends to the DO.
12. DO adjudicates and responds to all DRB comments and incorporates them into the directive using track changes.
13. Does the Directive meet the objective? The DRB votes to concur or non-concur with the document and recommendation to forward on to the Approving Official.
14. If the DRB votes to Non Concur, the directive is sent back to the DO for more work.
15. If the DRB votes Concur, a clean copy of the directive is prepared with required track changes incorporated and M&O prepares the Approval Package for signatures.
16. Approving Official signs the directive package.
17. M&O publishes the interim directive to the NIST internal website and updates the directives database.

APPENDIX B (continued)

18. M&O allocates 45 business days for OCC review. If no feedback is provided the directive goes final. If there is feedback, OCC will provide comments to the DO and M&O, the approving official will have the final determination.
19. M&O schedules the directive for the next DRB Review.

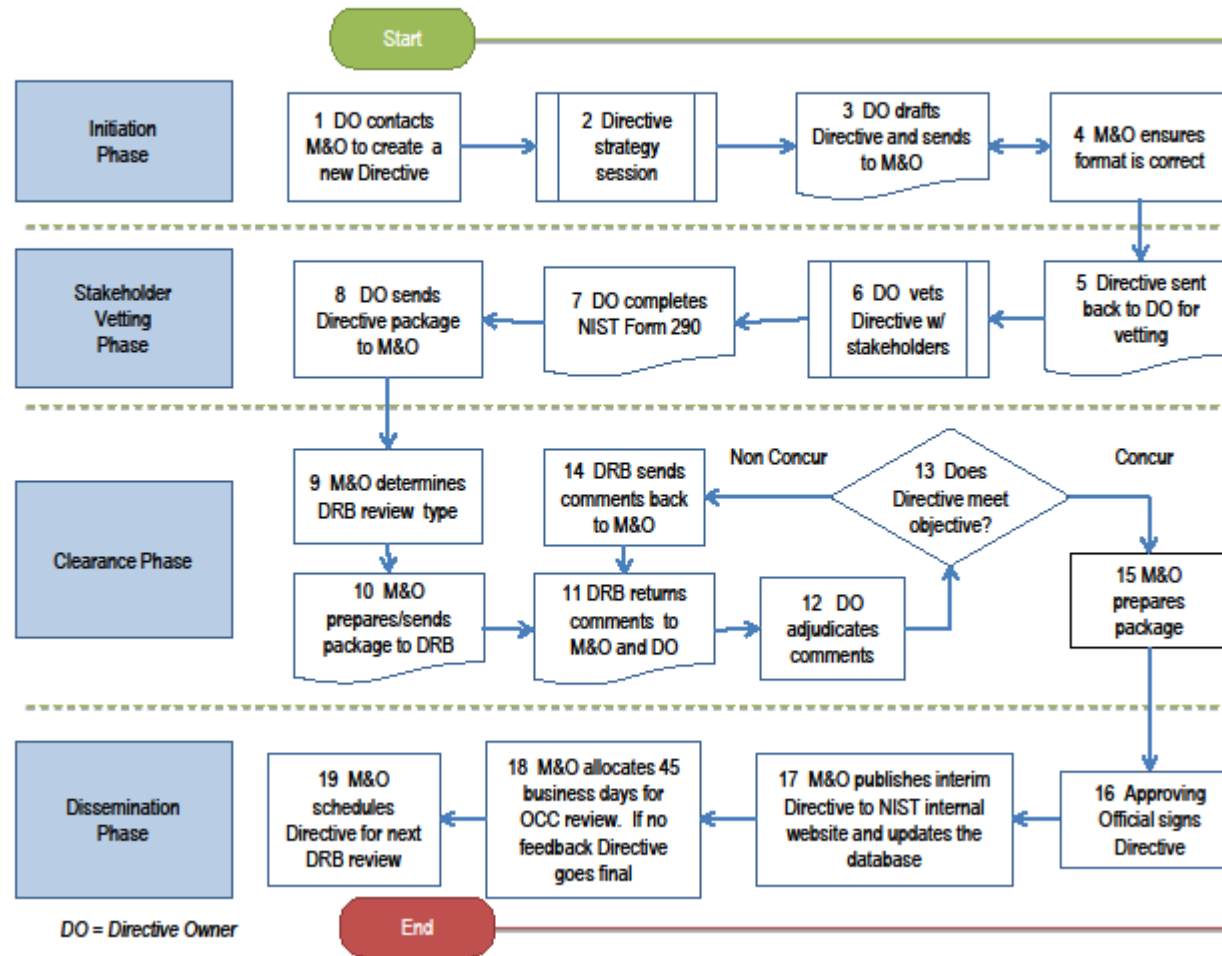
APPENDIX B (continued)

NEW DIRECTIVE PROCESS FLOW DIAGRAM

General Process Flow in relation to:

Directive Review Board (DRB) New Directive Process Flow

June 2014



APPENDIX B (continued)

Existing Directive Process Flow (Does not apply to suborders and guidance)

(Each number below corresponds to a specific block on the diagram):

1. Management and Organization (M&O) contacts Directive Owner (DO) to begin review of the directive. (see note below)
2. DO reviews directive.
3. Is the directive up to date?
4. If yes, M&O updates the directives database, the NIST internal website and schedules next review. Process ends.
5. If no, DO updates the directive.
6. DO vets directive with their NIST stakeholders/customers (legal as required).
7. DO updates the draft.
8. DO completes NIST Form 290 and sends the directive package to M&O.
9. M&O determines DRB review type.
10. M&O prepares and sends package out to the Directives Review Board (DRB) with comment sheet and clean version of the directive.
11. DRB members send comment sheet back to M&O, who consolidates the comments and sends to DO for adjudication.
12. DO adjudicates the comments and incorporates them into the directive using track changes.
13. Does the directive meet the objective? The DRB votes to concur or non-concur with the document and recommendation to forward on to the Approving Official.
14. If the DRB votes to 'Non Concur', the directive is sent back to the DO for more work.
15. If the DRB votes 'Concur', a clean copy of the directive is prepared with required track changes incorporated and M&O prepares the Approval Package for signatures.
16. Approving Official signs the directive package.
17. M&O publishes the interim directive to the NIST internal website and updates the directives database.
18. M&O allocates 45 business days for OCC review. If no feedback is provided the directive goes final.
19. M&O schedules the directive for the next DRB Review.

Note: Procedures are fully vetted by the DRB upon initial creation; all subsequent NIST-wide updates only require notification to the DRB.

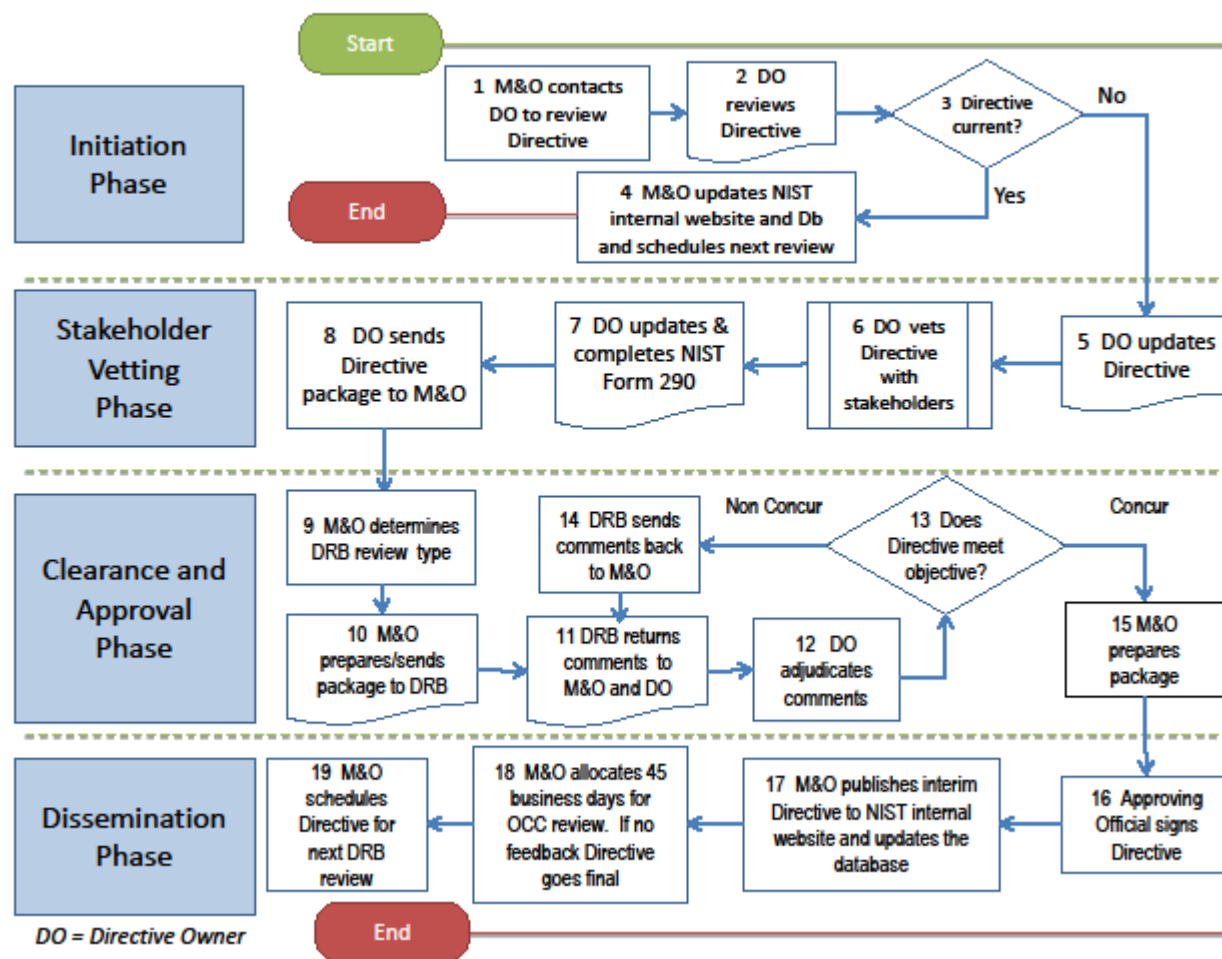
APPENDIX B (continued)

EXISTING DIRECTIVE PROCESS FLOW DIAGRAM (except suborders and guidance)

General Process Flow in relation to:

Directive Review Board (DRB) Update Existing Directive Process Flow

June 2014



APPENDIX C

APPENDIX C SUBORDER PROCESS

Suborders will not be formally reviewed by the Directives Review Board (DRB); an informational copy will be provided to all DRB members by Management and Organization (M&O).

Suborder review and approval process — Each Suborder must satisfy all of the following requirements:

- There must be a valid need for the information;
- The Directive Owner (DO) must have the means to support the documentation; and
- There must be:
 - An individual with the delegated authority to recommend approval to the approving official or
 - A chartered administrative committee with the delegated authority to recommend approval to the approving official.

The DO is responsible for completing the following process:

1. DO contacts Management and Organization (M&O) to create the new Suborder.
2. M&O and DO meet to discuss the new Suborder/strategy.
3. DO drafts a Suborder and sends to M&O.
4. M&O reviews the Suborder and ensures proper format.
5. Suborder is returned to the DO for NIST vetting.
6. DO vets the Suborder within their organization and stakeholders (legal as required) including the chartered Administrative Committee responsible for the Suborder.
7. DO sends the Suborder and NIST Form 290 package to M&O. NIST Office of Chief Counsel (OCC) and DRB clearance are not required. The executive Approval section must be completed and signed by the approving official designated in the Committee's charter.
8. M&O publishes the Suborder to the NIST internal website and updates the directives database.
9. M&O schedules the Suborder for announcement at the next DRB Review.

APPENDIX D

APPENDIX D GUIDANCE PROCESS

Guidance directives will not be formally reviewed by the Directive Review Board (DRB); an informational copy will be provided to all DRB members by the Management and Organization Office (M&O).

The directive owner is responsible for completing the following process:

1. Directive Owner (DO) contacts M&O to create the new guidance.
2. M&O and DO meet to discuss the new directive/strategy.
3. DO drafts a guidance and sends to M&O.
4. M&O reviews the draft guidance and ensures proper format.
5. Guidance is returned to the DO for NIST vetting.
6. DO vets new guidance within their organization and stakeholders (legal as required) and incorporates changes to the document.
7. DO sends vetted draft guidance and NIST Form 290 package to M&O. Office of the Chief Counsel for NIST and Directives Review Board clearance are not required. The NIST Form 290 must be signed by the approving official.
8. M&O publishes the guidance to the NIST Internal Website and updates the directives database.
9. M&O schedules the guidance for the next DRB Review.

APPENDIX E

APPENDIX E - DIRECTIVE NUMBERING

NIST requires the following specific directive alphanumeric structure be used to identify directives and make it easier to search and find information. The alphanumeric identifier for each directive shall have:

1. A letter identifying the type of document

P = Policy	O = Order	S = Suborder	PR = Procedure	G = Guidance	N = Notice
---------------	--------------	-----------------	-------------------	--------------	------------

2. A four-digit number identifying the subject category (see list below)

The following example illustrates the numbering system for directives:

NIST P 1100.00, *NIST Directives Management System*

“P” designates policy

First “1” designates the subject category (Administration and Analysis 1000 series, see below)

Second “1” designates the first policy in this subject category

“00” designates Order numbers

“.00” designates Suborders, Procedures and Guidance and Notices

Each document header will list the effective date, and the footer will contain the version number.

Subject Categories

The NIST DMS subject categories are:

1000 -Administration

This category contains those directives that cut across NIST programs and administration, including the many federal government compliance areas and day-to-day business.

Examples include:

Zero Tolerance Harassment Policy

Records/Forms Management

Audit Activity

2000 - Operations

This category contains all directives related to NIST daily and recurring operations, including facilities and property management. Examples include:

Site and Facilities Management

Emergency Management

APPENDIX E (continued)

Site Closure

3000 - Personnel

This category contains all directives specifically related to Human Resources functions.

Examples include:

Telework

Classification

Time and Attendance

4000 - Financial Management

This category contains all directives related to NIST financial resources, including budget, receivables, grants management and acquisition management. Examples include:

Travel

Gifts and Bequests

Cost Accounting

5000 - Scientific

This category contains all directives related to the NIST laboratory programs. Examples include:

Scientific Integrity

Patents and Inventions

Domestic Guest Researchers

6000 - Information Systems

This category contains all directives related to NIST Information Systems Management.

Examples include:

IT Privacy Program

Access and Use

Investigating Suspected Misuse of IT Resources

7000 - Safety

This category contains all directives related to NIST safety, including health, environment and radiation. Examples include:

Occupational Health and Safety

Ionizing Radiation Safety

Environmental Management

APPENDIX F

APPENDIX F - REVISION HISTORY

The revision history is included to provide a detailed listing of the changes that are occurring during this vetting period as well as providing a history of previous versions. Both the Directive Owner and the Management and Organization Office will update this table. The first version of the directive will contain a blank table. For the final published version, all current vetting detail will be deleted and only a history for that version retained.

Revision	Date	Responsible Person	Description of Change
Ver 1	12/8/2011	Dan Cipra (M&O)	Final Published Version
Ver 2.01	2/8/13	Dan Cipra (M&O)	Incorporated numerous substantive changes throughout the document.
Ver 2.02	3/27/13	Dan Cipra (M&O)	Numerous changes from Mike Herman as well as formatting changes.
Ver 2.03	9/9/13	Dan Cipra (M&O)	New Requirements section and new format.
Ver 2.04	11/13/13	Mike Moore	Review of final draft
Ver 2.05	12/4/13	Mike Herman	Review of final draft
Ver 2.06	1/7/14	Dan Cipra	Updated based on MM and MH reviews corrections updates.
Ver 2.07	2/4/14	Dan Cipra	Updated based on OCC Comments
Ver 2.08	2/26/14	Dan Cipra	Updated based on OCC Comments.
Ver 2.08	4/3/14	Dan Cipra	Incorporated OCC comments and changes.
Ver 2.09	5/6/2014	Dan Cipra	Made updates based on new DRB Charter, specifically the process flow for new and existing directives.
Ver 2.1	6/10/14	Dan Cipra	Incorporated all DRB comments in final.

Equal Employment Opportunity (EEO) and Diversity

NIST P 1200.00
Effective Date: 6/1/2011

PURPOSE

This directive prescribes the policy for the Equal Opportunity and Diversity Programs at the National Institute of Standards and Technology (NIST). NIST and the Department of Commerce are leading forces for economic growth. We foster the conditions for the nation's economic growth and opportunity by promoting innovation, measurement science, and collaborative standards development.

We recognize that in order to be successful as a federal agency, we must practice the principles of mutual respect and equal access to employment opportunities. As we continue to foster the conditions for technological innovation and economic development through robust standards, our commitment to the following principles will enhance our ability to carry out the mission of the agency.

SCOPE

This policy applies to all NIST employees.

LEGAL AUTHORITIES

- Title VII of the Civil Rights Act of 1964, as amended
- The Pregnancy Discrimination Act of 1978
- The Equal Pay Act of 1963 (EPA)
- The Age Discrimination in Employment Act of 1967, as amended
- Title I of the Americans with Disabilities Act of 1990 (ADA), as Amended (ADAAA)
- Sections 102 and 103 of the Civil Rights Act of 1991
- Sections 501 and 505 of the Rehabilitation Act of 1973
- The Genetic Information Nondiscrimination Act of 2008 (GINA)

POLICY

NIST does not tolerate discrimination based on race, color, religion, sex (including gender identity and sexual orientation), pregnancy, national origin, age (40 years of age and older), disability (including the provision of reasonable accommodation), genetic information, and participation in protected Equal Employment Opportunity (EEO) activities. These protections

encompass all aspects of employment, including recruiting, hiring, training, promotions, employee development, separations, and awards. Retaliation against those who initiate discrimination complaints, participate in any employment discrimination investigation or lawsuit, or otherwise oppose discrimination and harassment is strictly prohibited.

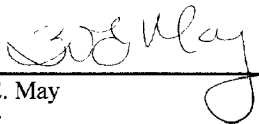
NIST managers and supervisors are responsible for preventing, documenting, and promptly correcting harassing conduct in the workplace. Managers should consult Department Administrative Order (DAO) 202-955, Allegations of Harassment Prohibited by Federal Law, and the NIST Office of Human Resources Management for additional guidance.

NIST staff who feel that they have been discriminated against on the job must contact an EEO Counselor or the NIST Civil Rights and Diversity Office within 45 calendar days of an alleged incident of discrimination to initiate a complaint. The NIST Civil Rights and Diversity Office may be reached by phone at 301.975.2038, by email at CRO@nist.gov, by mail at MS 1080, or in person at the Administration Building (Building 101), room A537 on the NIST Gaithersburg campus.

NIST seeks to resolve workplace conflicts in a prompt, impartial, confidential, nondiscriminatory, and constructive manner, without fear of reprisal. We encourage all NIST employees to use the Alternative Dispute Resolution (ADR) Program as a valuable tool in resolving Equal Employment Opportunity disputes.

NIST will continually strive to establish and maintain a workforce that reflects America's diverse populace and promotes an environment that respects and values individual differences. NIST recognizes that the ability to attract, develop, and retain a skilled workforce is key to the Institute's continued success and must be viewed and treated as a top priority.

Managers, supervisors, and employees should work together to support NIST's commitment to EEO and diversity. EEO and diversity are sound management practices, which help ensure that the best and brightest people are chosen and retained for a workforce that reflects the diversity of our nation.



Willie E. May
Director

2/4/16
Date

Visiting Researcher and Associate Policy

NIST P 1400.00
Effective Date: 9/8/2015

PURPOSE

The purpose of this policy is to outline the expectations under which visiting researchers and associates, hereinafter referred to as “individuals” are invited to collaborate with staff of the National Institute of Standards and Technology (NIST) and/or use facilities owned and/or operated by NIST. This policy further describes the goals to be achieved from such collaborations. Lastly, this policy assigns responsibility for carrying out various aspects of this policy to the most appropriate functional organizations at NIST.

SCOPE

This policy applies to all NIST employees, Organizational Units (OU), and offices that consider and approve requests from individuals from universities, other institutions, corporations, and non-U.S. organizations who wish to collaborate with NIST staff in programmatic areas of the Institute and/or use NIST facilities to conduct and/or observe research. All individuals must have appropriately documented NIST hosts while at NIST and shall not carry any official status of employment with NIST. In addition, unless legally permitted under their agreements with NIST, individuals representing or associated with non-Federal organizations may not perform the work of a NIST employee, nor can they officially represent NIST or the U.S. Government.

LEGAL AUTHORITY AND REFERENCES

- 15 U.S.C. 272(c)(5)
- 15 U.S.C. 272(c)(7)
- 15 U.S.C. 278g(a)
- U.S. Department of Commerce Administrative Order – DAO 207-12
- Export Administration Regulations (EAR) 15 C.F.R. §§ 730-774
- International Traffic in Arms Regulations (ITAR) 22 C.F.R. §§ 120-130

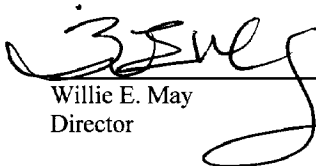
POLICY

NIST recognizes that individuals from universities, other institutions, corporations, and non-U.S. organizations may wish to visit NIST for extended periods of time for reasons including, but not limited to, conducting research in a NIST facility, collaborating with NIST researchers on specific projects of mutual interest, observing NIST staff research, and training with NIST staff on a measurement technique. NIST requires that such individuals be registered in the NIST

Visitor Registration System, that they undergo a background check when necessary, and that certain agreements between NIST, the individuals, and/or the individual's sponsoring institution be properly executed.

NIST requires that all hosts of visiting researchers and associates comply with and take into consideration all statutes, regulations and documents referenced in this policy and associated directives. Further, it is the policy that the extension of invitations to guest researchers and associates be based on the strategic interests of NIST and the Department of Commerce, rather than based on the goals and objectives of the visiting individuals, excepting some specifically prescribed circumstances in NIST's user facilities. Finally, the outcomes from collaborations with guest researchers and associates shall be mutually beneficial to both NIST and the visiting individual and/or their home organization. Unless otherwise indicated in an agreement or otherwise declared as proprietary, NIST hosts will inform associates that work products and research results from associates will be publically available.

The Director of the Technology Partnerships Office shall ensure the development of other directives necessary for the full and effective implementation of this policy for domestic guest researchers and associates while the Director of the International and Academic Affairs Office shall ensure the development of other directives necessary for the full and effective implementation of this policy for foreign guest researchers and associates.

 9/10/15

Willie E. May Date
Director

Foreign Visitors

NIST PR 1400.01
Effective Date: 8/20/2015

PURPOSE

This directive describes the procedures to be followed when inviting foreign nationals to visit NIST, making arrangements for such visitors, and preparing required reports. This document replaces Administrative Manual Subchapter 14.03.

APPLICABILITY

This directive is applicable to all NIST employees at NIST-Gaithersburg and NIST-Boulder.

REFERENCES

- Department of Commerce Administrative Order (DAO) 207-12
http://www.osec.doc.gov/opog/dmp/daos/dao207_12.html
- United States Department of State designated State Sponsors of Terrorism
<http://www.state.gov/j/ct/rls/crt/2011/195547.htm>
- IRS publication “Instructions for the Requester of Forms W-8BEN, W-8BEN-E, W-8ECI, W-8EXP, and W-8IMY” <http://www.irs.gov/pub/irs-pdf/iw8.pdf>

BACKGROUND

The International and Academic Affairs Office (IAAO) serves as the primary point of contact for all visits of foreign nationals to NIST. IAAO must be informed in advance of visits by foreign nationals. This procedure ensures NIST compliance with security, regulatory and other requirements of the Federal government including the Department of Commerce and the Department of State.

DEFINITIONS

Foreign National – any person who is not a citizen or national of the United States (U.S.) (including Permanent Residents/Green Card holders).

Foreign National Visitor (FNV) - a foreign national visiting a NIST site for three days or fewer, or attending a conference on a NIST site for five days or fewer. An FNV may not conduct research in NIST laboratories. To conduct such research, a foreign national must be registered as a NIST Associate in the NIST Associates Information System (NAIS).

Escort – a U.S. citizen employee of the Department of Commerce assigned the responsibility of accompanying a Foreign National Visitor who lacks authorized access within a NIST facility in order to ensure adherence to relevant security and safety measures, protecting classified,

Sensitive But Unclassified (SBU), or otherwise controlled, proprietary, or not-for-public release data, information, or technology from physical, visual, or virtual access.

Host/Sponsor - a U.S. citizen employee of NIST who is responsible for the day-to-day activities associated with the successful accomplishment of a foreign visit, including adherence to relevant safety and security measures and for taking all reasonable steps to protect classified, SBU, or otherwise controlled, proprietary, or not-for-public release data, information, or technology from unauthorized physical, visual, and virtual access by a Foreign National Visitor.

RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

NIST Director

- Delegates to the Director, IAAO, the authority to receive notices of visits to NIST of individuals from foreign countries. The IAAO Director will keep the NIST Director informed of visits determined to be of special interest.
- Delegates to the Emergency Services Division (ESD), in coordination with the Office of Security (OSY), the authority to approve site access for individuals from foreign countries.
- Delegates to the Associate Director for Laboratory Programs (ADLP), the authority to approve on a case-by-case basis the attendance of foreign nationals from countries designated as State Sponsors of Terrorism (<http://www.state.gov/j/ct/rls/crt/2011/195547.htm>) at conferences and meetings in the NIST public conference rooms and auditoriums.

IAAO Director

- Serves as the primary point of contact for FNVs, especially those who have had no prior contact with NIST employees; ensures that external protocol requirements are met; arranges appointments as appropriate; provides escort, and ensures adherence to relevant safety and security measures for visiting delegations at NIST when the visit is coordinated by IAAO; and assists visitors with arrangements as required.
- Advises FNVs hosted by IAAO that an Official Passport, Diplomatic ID Card or Permanent Resident Card/Green Card (if applicable) is required for entry onto the NIST sites. Except where responsibility is assumed by another NIST Organizational Unit (OU), IAAO has the lead responsibility for ensuring the coordination of all elements associated with the visit by an FNV.
- Maintains records of FNVs, including names, home institutions, date of visit and visit agenda for reporting purposes.
- Checks visa status for FNVs receiving lecture fees to determine eligibility of receiving NIST funds.

- Provides NIST Host/Sponsor with the following IRS publication “Instructions for the Requester of Forms W-8BEN, W-8BEN-E, W-8ECI, W-8EXP, and W-8IMY” <http://www.irs.gov/pub/irs-pdf/iw8.pdf> and informs hosts of their obligation to collect appropriate W-8 tax forms for FNVs receiving lecture fees.

Office of Security (OSY)

- Reviews information entered into the Visitor Registration System and processes the request for entry of FNVs onto the NIST site.
- Provides Counterintelligence Awareness Training to NIST staff in advance of their sponsoring any FNV and annually thereafter. The briefing may be found in the [NIST Commerce Learning Center](#) under NIST-specific training for "Counterintelligence Awareness". One-on-one training is also available from OSY on an as-needed basis upon request.
- Reviews and approves, on a case-by-case basis Memos for approval to the ADLP regarding attendance of foreign nationals from countries designated as [State Sponsors of Terrorism](#) at conferences and meetings in the NIST public conference rooms and auditoriums.
- During the course of a visit by, or upon the departure of select Visitors, particularly those from countries designated as State Sponsors of Terrorism, the servicing security office or OSY Headquarters may conduct a debriefing of the Host/Sponsor and/or other employees who have had contact with the Foreign National.

Emergency Services Division (ESD)

- Controls FNV access onto the NIST site.
- Issues Visitor passes at the Visitor Center.

Host/Sponsor

- The NIST primary host/sponsor must complete the Counterintelligence Awareness Training prior to sponsoring their first FNV, and annually thereafter.
- Registers FNVs in the [NIST on-line Visitor Registration System](#), at least 72 hours in advance.
- Advises FNV that an Official Passport, Diplomatic ID Card or Permanent Resident Card/Green Card (if applicable) is required for entry to the NIST site.
- Provides escort as necessary for visitors on the NIST site and ensures adherence to relevant safety and security measures.
- With management approval, provides official letters of invitation to FNV's coming from abroad and advises the FNV of the need to enter the U.S. on a Business Visa (B1 or WB).
- Provides any FNV receiving a lecture fee from NIST with [IRS Form W-8BEN](#). *A FNV with a tourist visa (B2 or WT visa) is not eligible to receive payment*
- Advises FNV of their obligation to determine whether an IRS W-8BEN form needs to be completed prior to receiving payment.

- Collects appropriate IRS W-8BEN form prior to issuing payment.
- If no IRS W-8BEN is received, Host/Sponsor is responsible for ensuring that NIST withholds 30% of payment for taxes and for entering payment information, including tax withholding amount into the Accounting Code Classification Structure (ACCS).
- Once payment is made, the Host/Sponsor sends completed IRS W-8BEN form to the NIST Finance Accounts Payable Office with a copy of the check.

Finance Division

- Maintains IRS W-8 BEN forms from FNVs receiving lecture fees.
- Makes the tax payment using the ACCS that was used to pay the guest speaker.

PROCEDURES

- With the exceptions listed below, and in accordance with DAO 207-12, NIST employees may invite FNVs to NIST and may make arrangements for the visit, requesting assistance from IAAO as needed.
- All FNVs must be registered via the on-line Visitor Registration System - <https://iapps.nist.gov:7100/Visitor/appLogin.html>, at least 72 hours in advance.
- All FNVs must present an Official Passport, Diplomatic ID Card or Permanent Resident Card/Green Card at the Main Gate/Visitor Center prior to entering the NIST site.
- Visitor passes are issued at the Visitor Center and may not exceed five (5) days in duration.

Foreign National Visitors Receiving Lecture Fees from NIST

- The NIST-1260 form, Report of Foreign Visitor(s), Guest(s), Conference Attendee(s) is required when a lecture fee, travel or per diem is requested for the FNV. The form must be sent to IAAO for approval at least seven working days in advance of the visit.
- If an FNV is already in the U.S., the NIST Host/Sponsor must send copies of the photo page of the FNV's current passport and visa used to enter the U.S. to IAAO, by fax or encrypted email, with the NIST-1260.
- If an FNV is arriving from outside the U.S. and will be receiving lecture fees, the NIST Host/Sponsor is required to provide an official letter of invitation. The FNV must present the official letter of invitation to the U.S. immigration officer at the port of entry into the U.S. to have their passport correctly stamped/marked for business (B1 or WB visa).
- IAAO will determine visa eligibility upon arrival at NIST. ***A FNV with a tourist visa (B2 or WT visa) is not eligible to receive payment.*** Current NIST foreign guest researchers are not eligible to receive lecture fees.

- IAAO will provide the NIST Host/Sponsor with the following IRS publication <http://www.irs.gov/pub/irs-pdf/iw8.pdf> to send to the FNV.
- The FNV is responsible for making the determination of which particular IRS W-8 form needs to be completed. The NIST Host/Sponsor must receive the appropriate IRS W-8 form prior to issuing payment.
- The completed IRS W-8 form must be collected and filed with Division issuing the check.
- If changes to the originally submitted NIST-1260 are necessary, a revised NIST-1260 must be submitted to IAAO. If the visit is cancelled, IAAO must be notified in advance of the scheduled date, if possible.

Visitors for Whom Special Clearance and Procedures are Required

- Visitors from Countries of State Sponsors of Terrorism- It is NIST policy that no access be permitted to NIST laboratory facilities by nationals of countries which have been designated as [State Sponsors of Terrorism by the U.S. Department of State](#) unless they are U.S. Legal Permanent Residents (LPRs)/Green Card holders. However, on a case-by-case basis, foreign nationals from these countries, who are not U.S. LPRs/Green Card holders, may be able to attend conferences and meetings in NIST public access areas with prior approval of the ADLP.
 - a. Invitations to Visit - Prior approval is required before an invitation to a citizen of a State Sponsor of Terrorism to visit NIST may be extended. When considering such an invitation, please contact IAAO.
 - b. Procedures for Receiving Visitors from Countries of State Sponsors of Terrorism – Host/Sponsor prepares a memorandum for approval addressed to ADLP through OU Office, the Director of IAAO, and OSY which must include following:
 - full name (as it appears on passport)
 - social security number (if applicable)
 - passport number and issuing country
 - visa number
 - date of birth (month, day, year)
 - place of birth (city and country)
 - citizenship
 - country of residence
 - countries of dual citizenship (if applicable)
 - national ID number
 - current employer (name, organization, and address)
 - purpose of visit / justification for visit

- topic of discussion at conference or meeting (a description of the subject matter and a statement on the potential for disclosure of sensitive information (e.g. classified, SBU, proprietary, export controlled, etc.))

A hard copy or encrypted email copy of the memorandum must be received by the ADLP at least 30 days prior to the proposed visit. The memorandum should not be sent by e-mail, unless the e-mail is encrypted. The NIST primary Host/Sponsor must complete Counterintelligence Awareness Training prior to the visit and may be required to undergo a debriefing by OSY during or following the visit.

If approved, [NIST on-line visitor registration](#) is required.

c. Conduct of the Visit - Visitors from the countries of State Sponsors of Terrorism must be accompanied by an assigned escort at all times while at NIST.

d. Non-NIST Sponsored Events - The procedures outlined in this section also apply to conferences held at NIST even when NIST hosts such conferences on behalf of other organizations. The NIST employee who initially extended the invitation to the Visitor from a State Sponsor of Terrorism to attend the conference is responsible for ensuring conformance with these procedures. IAAO must be notified immediately of visitors from the countries that have been designated as State Sponsors of Terrorism by the U.S. Department of State (as explained in the section above) who register for conferences at NIST or who come to NIST without previous notification of their visit.

DIRECTIVE OWNER

109 –International and Academic Affairs Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	10/13/12	Joy Foster (OIAA)	Original Draft from Admin Manual 14.03
Rev. .01	12/13/12	Dan Cipra (M&O)	Reformatted to DMS template
Rev. .02	1/17/13	Claire Saundry	Revised text Circulated to ESD, OSY and Finance for review
Rev. .03	2/19/13	Joy Foster	Revised to include ESD, OSY and Finance Comments. Text sent to M&O
Rev. .04	3/12/13	Dan Cipra	Formatting changes only.
Rev. .05	10/22/15	Dan Cipra	Incorporated OCC Interim Review edits

Domestic Associate Program

NIST O 1401.00
Effective Date: 10/5/2015

PURPOSE

This directive establishes requirements for administrative processing and hosting of domestic associate (DA) assignments; defines responsibilities of various NIST offices involved; and establishes the conditions under which a DA may be invited to work at NIST. This directive, together with NIST PR 5001.01, replaces Administrative Manual Subchapter 5.13.

APPLICABILITY

This directive applies to all NIST employees involved with the administrative processing and hosting of DAs at NIST sites including Gaithersburg, MD, Boulder, CO, and Hollings Marine Laboratory, Charleston, SC.

LEGAL AUTHORITIES AND REFERENCES

- [5 CFR 334](#)
- [15 CFR 256](#)
- [Federal Property and Administrative Services Act of 1949 \(FPASA\)](#), [40 U.S.C. 471-514](#) and [41 U.S.C. 251-260](#)
- The [Federal Acquisition Regulation \(FAR\) Title 48](#) of the Code of Federal Regulations
- [31 U.S.C. 6301-6308](#)
- [U.S. Department of Commerce Manual of Security Policies and Procedures](#)
- [Department Administrative Order 202-311 Voluntary and Uncompensated Services](#)
- Federal Travel Regulation System, [41 CFR 300-304](#)
- Visiting Researcher and Associate Policy NIST P 1400.00
- The Use of the Emeritus Title, NIST [N 1081.00](#) – See attached link for more detail.

FORMS

- [Visitor Registration Form](#)
- [NIST-1296, Domestic Associate Agreement](#) (Must be completed within the [NAIS system](#).)
- [Associate Summary](#)
- [NIST-351, Request for Federal Credential or NIST Site Badge](#)
- [DN-45, Invention Disclosure and Rights Questionnaire](#)

BACKGROUND

A Domestic Associate (DA) is any non-employee who is a U.S. citizen, comes to a NIST campus and/or uses NIST information technology (IT) resources, and is either working in a lab (for any period of time) or will be on campus for more than ten working days.

Listed below are DA Types (Click [here](#) for full descriptions):

Domestic Guest Researcher Research and Science (DGRRS)

Domestic Guest Researcher Technical (DGRTEC)

Domestic Guest Researcher Special Programs (DGRSPL)

Facility User (FU)

Intergovernmental Agency Personnel Act (IPA)

Non-Technical Support Personnel (NTSP)

Research Associate (RA)

Sole Proprietor Contractor (CON)

Volunteer Student (VOL)

Off-site Collaborator (COLLAB)

Other (OTH)

REQUIREMENTS

- NIST shall make its facilities available for qualified DAs to pursue scientific or technical projects under conditions determined by NIST.
- A NIST-1296 must be approved and signed by all parties before the DA uses NIST facilities and equipment to conduct research.
- A DA may not perform the work of a NIST employee.
- A DGR may not participate in a Cooperative Research and Development Agreement (CRADA) or in other NIST activities involving proprietary

information unless the proper exception from the NIST Technology Partnerships Office (TPO) has been obtained.

- National Center for Neutron Research (NCNR) FUs shall follow the requirements of NCNR processing.
- NIST shall not pay for the training of DAs for general work that is not specifically NIST-related training.
- DAs shall be required to follow directives related to occupational safety, health and environment.

Processing

- All DAs must be entered into and processed through the [NIST Associates Information System \(NAIS\)](#).
- Using NAIS, Form [NIST-1296](#) or [Associate Summary](#) must be prepared for any U.S. citizen performing work at NIST.
- For entry on the NIST campus, the host must enter the DA into the NIST on-line [Visitor Registration](#) system prior to their arrival. This can be done through NAIS.

Security

- A DA must meet all NIST security requirements.
- Security forms shall not be required if a DA is working at NIST for thirty days or less. In NAIS, use the security-opt-out process. In compliance with the U.S. [Department of Commerce Manual of Security Policies and Procedures 11.3.E](#), such individuals must be escorted at all times.
- A DA will not be issued a NIST site badge, allowed access to an IT account, or provided with a NIST telephone extension without being processed through NAIS.
- The Office of Security (OSY) will check for any prior background investigations. If necessary, OSY will fingerprint the DA and process the required security paperwork. Once processing is completed, the DA will be given a site access badge.

Travel

- Domestic Associates (DA) may travel under specified conditions.
- NIST will only pay for travel related to the DAs work under a funding agreement (e.g. contract or grant) may only travel under the terms of their agreement.
- DAs working under a funding agreement (e.g. contract or grant) may only travel under the terms of their agreement.

- DAs working under a Cooperative Research and Development Agreement (CRADA) may travel only as specified in the agreement (e.g. the NIST CRADA with the Standard Alumni Associate addresses travel).
- DAs are prohibited from performing NIST work, so invitational travel outside of an agreement or other authority is not permitted.

RESPONSIBILITIES

Domestic Associate

- Provides information necessary to complete NAIS (Form [NIST-1296](#) or [Associate Summary](#) and security paperwork as required);
- NIST 1296 form must be signed by DGRs and RAs after arrival;
- Provides security paperwork to security office to obtain badge;
- Participates in orientation provided by Office of Human Resources Management (OHRM). Orientations in Boulder are conducted by each OU.
- NCNR FUs follow the requirements of NCNR processing;
- Obeys U.S. Federal employee and NIST conduct rules including IT security and Safety, and NIST Directives applicable to DAs;
- A DA agrees to disclose to NIST, using Form [DN-45, Invention Disclosure and Rights Questionnaire](#), any inventions conceived or made during the course of the project. Joint inventions will be jointly owned. Sole inventions will be owned by the inventing party. Unless superseded by written agreement executed prior to conception of an invention, NIST reserves the right to a nonexclusive, nontransferable, irrevocable, paid-up license to practice or have practiced for on behalf of the United States Government any subject invention throughout the world. Software and data prepared solely by NIST employees, prepared jointly by NIST employees and the DA, or prepared solely by the DA, shall not be copyrighted and shall be placed into public domain for unrestricted dissemination.

Host Division

- Adheres to the assignment and administrative procedures applicable to the NIST DA Program;
- Assigns a host for the DA;
- A DA must obey all applicable NIST directives to the extent allowed by law and the terms of the Associate's agreement. Hosts are responsible for communicating these applicable requirements to the DA;

- Defines or accepts the project and/or research objectives, the relevance of the scope to the mission of the host division, and schedule of work;
- Determines if DA is working under the auspices of a NIST funding agreement;
- Appropriately classifies the DA in NAIS according to the intended scope of work and with consideration of the appropriate level of access to NIST assets and information;
- Processes all required forms through NAIS, and forwards through the OU for approval;
- Prepares security paperwork as required;
- Enters DA into the NIST on-line [Visitor Registration](#) system prior to their arrival. Once a DA has been registered in NAIS, all visits should be submitted to the on-line Visitor System via the NAIS Visitor Registration feature.;
- Ensures the DGR or RA signs the [NIST-1296](#). The form may be signed in the host division, and scanned and attached to the NAIS process. In Gaithersburg, the host division has the option of allowing the signature collection to be completed in TPO Onboarding;
- Enters the DA arrival date into NAIS. If the [NIST-1296](#) is signed in the host division, the scanned form is attached to the NAIS process;
- Provides safety orientation; and assures the DA attends the orientation provided by OHRM. At Boulder, NIST Associates orientation is not conducted;
- Informs DA of the obligation to conform to the usual administrative requirements and rules of conduct generally applicable to NIST employees including protection of human and animal subjects;
- Ensures compliance with on-boarding and off-boarding processes;
- Provides technical guidance to DA as appropriate.

Organizational (OU) Director or Delegate

- Reviews and approves the NAIS process, including Form [NIST-1296](#) and [Associate Summary](#), and description of work to be performed for suitability and eligibility;
- Forwards approved forms through NAIS to TPO with supporting documentation as necessary.

- Ensures that travel is limited to the approved scope of an agreement.
- Plans needed travel into the scope of agreements (e.g. contracts, grants, CRADAs).

Technology Partnerships Office (TPO) Director or Delegate

- Manages the NIST DA Program;
- Reviews and negotiates modifications to Form [NIST-1296](#) to ensure completeness and accuracy;
- Approves completed Form [NIST-1296](#);
- Responds to inquiries concerning the NIST DA Program;
- Provides alternative support to the host division for obtaining DA signature;
- Sponsors DAs in US Access System for PIV badge.

NIST Office of Security (OSY)

- Reviews security investigation requests for completeness and accuracy and submits to the Office of Personnel Management;
- Checks for any prior investigations before initiating a new investigation;
- Fingerprints the DA, if necessary;
- If requested, approves after-hours access once security investigation is complete;
- Notifies the appropriate OUs regarding security investigations;
- Adjudicates favorable investigations.

Emergency Services Division (ESD)

- Uses Form [NIST-351, Request for Federal Credential or NIST Site Badge](#), in NAIS to prepare and issue a NIST site badge.

Office of Information Systems Management (OISM)

- Provides access to servers and maintains data files for NAIS.

DIRECTIVE OWNER

401 - Technology Partnerships Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Revised Draft	7/29/14	Mary Clague	Revised Draft
Initial Draft	6/18/2012	Mary Clague	Initial Draft
Rev. .01	6/27/2012	Dan Cipra	Formatting changes only.
Rev. .02	12/12/12	Dan Cipra	Removed Procedures section and created a new directive.
Rev. .03	6/22/15	Brenda Thomasson	Reviewed draft

Use of the Emeritus Title

NIST N 1401.01
Effective Date: 10/25/2013

PURPOSE

This notice establishes the requirements and responsibilities for the use of the emeritus title for retired Federal Staff of the National Institute of Standards and Technology (NIST). This notice replaces Administrative Manual 5.13 Domestic Guest Researchers Appendix C.

APPLICABILITY

This notice applies to NIST-Gaithersburg and NIST-Boulder.

AUTHORITIES AND REFERENCES

- 15 U.S.C. § 272(c)(7)
- Department Administrative Order 202-311 Voluntary and Uncompensated Services
- Federal Travel Regulation System, 41 CFR Parts 300-304

BACKGROUND

Organizational Unit (OU) Directors may grant the “Emeritus” title to retirees from their organizations who continue to work with NIST as a guest researcher and meet certain criteria. Titles include, but are not limited to, “Scientist Emeritus” and “Engineer Emeritus.” These are considered highly distinguished titles and should be used to denote both an exceptional level of past accomplishment and the ability to actively continue to contribute to the on-going mission of NIST. This authority may not be re-delegated below the OU Director level.

REQUIREMENTS

- An individual granted the Emeritus title by a Laboratory Director must meet all of the following criteria:
 1. Is a retired NIST employee.
 2. Has a distinguished record of accomplishment, as determined by the OU Director, including consideration of significant technical achievements, publications, talks, committee activities, honors, and awards - especially in the most recent two-year period.
 3. Possesses the desire and ability to actively and prospectively perform scientific and/or technical work that complements the mission of the OU, as determined by the OU Director.
- An individual granted the Emeritus title by a Management Resources or Industry and Innovation Services OU Director must meet all of the following criteria:
 1. Is a retired NIST employee.

2. Has a distinguished record of accomplishment, as determined by the OU Director, including consideration of past service to NIST, expertise and leadership within their field, committee activities, honors, and awards - especially in the most recent two-year period.
 3. Possesses the desire and ability to actively and prospectively support the delivery of NIST services through work that complements the mission of the OU, as determined by the OU Director.
- Emeritus individuals are processed in the NIST Associate Information System (NAIS) and must abide by all laws, regulations and policies governing Domestic Guest Researchers at NIST. While Emeritus individuals shall not perform governmental functions, such as directly representing NIST, they may collaborate with NIST scientists in areas of mutual interest, mentor young scientists, provide individual expert guidance and advice regarding their area of technical expertise, facilitate and foster collaborations between NIST and other organizations, and perform other similar activities.
 - The Emeritus title may be granted for a period of up to two years and may be renewed as long as the selection criteria continue to be satisfied.
 - The NIST Director will recognize the Emeritus individual in a congratulatory letter, and the OU will provide him or her with a certificate. The letter of recognition and certificate will not be reissued for each two-year renewal.

RESPONSIBILITIES

NIST Director: -

- Sends the Emeritus individual a congratulatory letter (see Appendix B)

OU Director –

- Determines eligibility for candidates
- Grants Emeritus Status for eligible candidates
- Provides selected Emeritus individuals with a certificate (See Appendix C)

OU Division Chief –

- Nominates candidates for Emeritus title to the OU Director (See Appendix A)
- Ensures NIST Form 1296 is completed and signed by the candidate
- Ensures that the Emeritus individual does not perform government functions.

DIRECTIVE OWNER

410 – Technology Partnerships Office

APPENDICES

- A. Sample Designation Memorandum
- B. Sample Congratulatory Letter
- C. Sample Certificate
- D. Revision History

APPENDIX A

SAMPLE DESIGNATION MEMORANDUM

(Date)

MEMORANDUM FOR: (Name)
Director, NIST

From: (Name)
Director, (OU)

Subject: Request for (Select: Scientist, Engineer, etc.) Emeritus Status for (Emeritus Name)

I have determined that (Emeritus Name) has met the NIST criteria to receive the title of NIST (Select: Scientist, Engineer, etc.) Emeritus and request you sign the attached congratulatory letter noting this prestigious designation. (Emeritus Name) retired from NIST in (Insert year) and I have determined that his/her distinguished record of accomplishment and service has merited this designation. The (Insert OU) will continue to benefit from the active participation of (Emeritus Name) in collaborating in areas of mutual interest, mentoring young scientists, and providing expert guidance and advice.

cc: (Associate Director)
(Division Director)
Technology Partnerships Office

APPENDIX B

SAMPLE CONGRATULATORY LETTER

(Date)

(Emeritus Name)

National Institute of Standards and Technology

(Division)

(Address)

Dear (Emeritus Name):

Congratulations on your appointment as (Select: Scientist, Engineer, etc.) Emeritus at the National Institute of Standards and Technology. This appointment is effective (date) for a term of 2 years. Your appointment is sponsored by (division) of the (OU).

The position of (Select: Scientist, Engineer, etc.) Emeritus is held by some of NIST's most illustrious alumni. It is awarded to those who have a distinguished record of achievement and wish to remain actively engaged with NIST in their retirement. An Emeritus may collaborate with NIST employees in areas of mutual interest, mentor young employees, provide individual expert guidance and advice regarding their area of technical expertise, facilitate and foster collaborations between NIST and other organizations, and similar activities.

We are proud of your accomplishments at NIST and are confident that you will continue to contribute to our mission. We appreciate your many years of service as a member of the NIST staff, and wish you continued success in your endeavors.

Sincerely,

(Name)

NIST Director

cc: (Associate Director)

(OU Director)

(Division Director)

APPENDIX C

SAMPLE CERTIFICATE

Certificate of Appointment

to the Position of

(Select: Scientist, Engineer, etc.) Emeritus

(Insert: Lab/OU)

National Institute of Standards and Technology

Conferred Upon

(Insert: Name)

*To recognize outstanding accomplishments
and leadership and to foster continued
support of the (Lab/OU) mission.*

(Lab/OU Director Name)

(Lab/OU)

(Date)

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

APPENDIX D

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	6/3/13	Dan Cipra	Initial Draft
Ver .01	6/4/13	Dan Cipra	Incorporated OCC changes
Ver. .02	6/18/13	Mary Clague	DRB comments and suggestions incorporated.
Ver .03	10/18/13	Dan Cipra	Removed PMB Responsibility per OCC and OWM direction. Informed DO.
Rev. .04	10/29/2015	Dan Cipra	Updated Directive Number

Domestic Associates Program Procedures

NIST PR 1401.01
Effective Date: 10/5/2015

PURPOSE

This directive establishes procedures for administrative processing and hosting of domestic associate (DA) assignments, including use of the NIST Associates Information System (NAIS), and defines the responsibilities of various NIST offices involved. NIST PR 1401.01, together with NIST O 1401.00 replaces Administrative Manual Subchapter 5.13.

APPLICABILITY

The procedures outlined in this directive apply to all NIST employees involved with the administrative processing and hosting of DAs at NIST sites including Gaithersburg, MD, Boulder, CO, and Hollings Marine Laboratory, Charleston, SC.

REFERENCES

- NIST P 1400.00 Visiting Researcher and Associate Policy
- NIST O 1401.00 Domestic Associates Program

FORMS

- [Visitor Registration Form](#)
- [Form NIST-1296, Domestic Associate Agreement](#) (Must be completed within the [NAIS system](#).)
- [Form NIST-351, Request for Federal Credential or NIST Site Badge](#)
- [Form NIST-1221, Telecommunication Service Request and Directory Information](#)
- [Boulder Access Request Form](#)
- [Form DN-45, Invention Disclosure and Rights Questionnaire](#)
- [Form NIST-1251, Hazardous Materials Clearance for Nonemployees](#)
- [Form NIST 1284, Access Change Request](#)

PROCEDURES

I. Pre-arrival of Domestic Associate

- The Gaithersburg and Boulder Arrival Checklists (available at <https://inet.nist.gov/tpo/services/nais-templates-and-forms>) outline the activities and steps required for Associate on-boarding (agreement preparation and associate arrival).
- Host division is responsible for data collection (forms and templates are available [here](#)) from potential DAs and entering information into NAIS. NAIS will automatically generate required forms and appropriate routing for approval.
- Instructions on the NAIS system, including user guides and tutorials, may be found [here](#).
- Using NAIS, the host division prepares the appropriate form ([Form NIST-1296](#) or [Associate Summary](#)):
 1. Determines the length of time for the DA agreement;
 2. Develops a work plan and description of the work to be accomplished or accepts the work plan of a contract, grant, cooperative agreement or simplified acquisition;
 3. Determines if the DA is working at NIST under the auspices of a NIST funding agreement and states the type and number of the funding agreement using NAIS;
 4. Establishes the need for security investigation;
 5. Determines the need for after-hours access;
 6. Identifies in NAIS when information technology (IT) account is needed; and
 7. Submits all appropriate forms through NAIS for approval.
 8. Security Investigation Requirements:
 - Descriptions of investigation requirements for non-federal employees is available in Section 11.3 of the [DoC Manual of Security Policies and Procedures](#). OSY will determine the appropriate investigation based on information provided in NAIS.
 - If the length of stay is thirty working days or less within a calendar year, a security investigation is not required. (In NAIS, use the security-opt-out process.) These DAs must be escorted at all times.
 - If the length of stay is greater than thirty working days within a calendar year, the host division prepares and submits the required security forms in

NAIS. An escort will be required until a satisfactorily completed security investigation' obtained.

- Security forms are prepared in NAIS prior to DA's arrival at NIST. The DA must submit these forms to the Office of Security (OSY) within three working days after their arrival at NIST and if applicable, complete the eQIP process.
- Host division is responsible for entering DA's information into the NIST on-line [Visitor System](#) prior to scheduled arrival date. Once a DA has been registered in NAIS, all visits should be submitted to the on-line Visitor System via the NAIS Visitor Registration feature.
- Unescorted out-of-hours access to the NIST site is contingent upon a satisfactorily completed security investigation. For out-of-hours approval, the host division initiates an Update process in NAIS and changes the requested access level.

II. Arrival of the Domestic Associate

- A representative of the host division meets the DA and enters the actual arrival date in NAIS.
- The host division ensures the DA's personal information matches two forms of ID. Domestic Guest Researchers (DGR) and Research Associates (RA) must sign the [NIST-1296](#) either in the host division or Technology Partnerships Office (TPO) Onboarding (Gaithersburg only). If in the host division, the scanned form is attached to the NAIS process.
- **NIST Center for Neutron Research (NCNR) Facility Users (FU)** follow the requirements of NCNR processing.
- If the security forms were not completed prior to arrival, the host division must ensure that the DA completes security forms and schedules an appointment with OSY within 3 working days.
- OSY meets with DA, takes fingerprints if needed, ensures that all security forms have been submitted and filled in correctly, submits paperwork for investigation, and authorizes a NIST site badge. Once the investigation has been completed and adjudicated, OSY approves Form [NIST-1284](#) for after- hour's access, if previously requested. At NIST Boulder, the host collects all required information and forwards to OSY.
 - The Fingerprint form is mailed to the OSY office.
 - The remaining security forms in the NAIS package are attached to the NAIS process.

- In Gaithersburg, the Emergency Services Division (ESD) uses Form [NIST-351](#) in NAIS to prepare and issue a NIST site badge. In Boulder, the [Access Request Form](#) is required to issue a NIST site badge.
 - NAIS will forward the NIST-351 to ESD for both Gaithersburg and Boulder when OSY has authorized the issuance of a site badge.
 - The Access Request Form must be completed outside of NAIS in Boulder and the completed form with the appropriate signatures must be taken to ESD when the DA gets their Badge
- Supervisors shall follow Organizational Unit (OU)-established policies and procedures regarding the safety training of new DAs.
- The host division reviews procedures and guidelines and prepares Form [NIST-1221](#), if applicable.
- The host division, as necessary, identifies workspace, prepares desk and computer setup, provides office key(s), assists in obtaining IT accounts, and assigns a NIST employee to escort the DA until he/she has been issued a NIST site badge.
- At Gaithersburg, the host division makes arrangements through OHRM for DA to attend orientation on the [Commerce Learning Center website](#). Orientation is conducted by the OU in Boulder.

III. Departure of a Domestic Associate

- The host division enters the DA's actual departure date in NAIS.
- Departure checklists are available [here](#). These are required by O 3114.00 Associate Entrance on Duty and Separation Clearance and must be kept for a period of one year after DA departure.
- The following actions are taken when applicable:
 - Host division prepares [Form NIST-1251](#), Hazardous Materials Clearance for Nonemployees.
 - Host division collects key(s) and NIST site badge from the DA. The host division returns keys and NIST site badge to appropriate NIST offices.
 - Host division informs DA that all library material must be returned to the NIST Research Library and is responsible for materials loaned to the DA. At NIST Boulder, library material must be returned to the Boulder Laboratories Library.

- Host division closes IT Accounts and transfers NIST property (laptop/computer, cell phone, etc.).
- NCNR FUs follow the requirements of NCNR processing.

IV. Extension of a Domestic Associate Assignment

- Using NAIS, the host division prepares and submits through the OU a NAIS process, marking the “Agreement” block as an extension. The host division submits the NAIS process through the approval process.
- The host division and DA follow the arrival process for [NIST-1296](#) signature and badge extension.

V. Cancellation of a Domestic Associate’s Appointment Prior to Arrival

- Using NAIS, the host division cancels the associate agreement, which notifies appropriate offices.

DIRECTIVE OWNER

401 - Technology Partnerships Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Revised Draft	7/29/14	Mary Clague	Revised Draft
Rev .01	6/22/2015	Brenda Thomasson	Reviewed draft
Rev. .02	9/9/2015	Mary Clague	Updated based on DRB Comments

Foreign Guest Researcher Program

NIST O 1402.00
Effective Date: 5/26/2015

PURPOSE

This directive establishes NIST requirements for administrative processing and hosting of Foreign Guest Researchers (FGRs); defines responsibilities of various NIST offices involved; and establishes the conditions under which a FGR may be invited to conduct research collaboratively at NIST. This order, together with NIST PR 1402.01 replaces Administrative Manual Subchapter 5.14.

APPLICABILITY

This directive applies to all NIST employees involved with the administrative processing and hosting of Foreign Guest Researchers at NIST including NIST Gaithersburg, MD, NIST Boulder, CO, Hollings Marine Laboratory, and Charleston, SC

LEGAL AUTHORITIES AND REFERENCES

- [15 U.S.C. 272\(c\)\(5\)](#)
- [15 U.S.C. 278g\(a\)](#)
- [22 CFR Part 62 Exchange Visitor Program](#)
- [U.S. Department of Commerce Administrative Order – DAO 207-12](#)
- P 1400.00 Visiting Researcher and Associate Policy
- [IRS publication 515](#) (withholding Tax on Non-resident Aliens and Foreign Entities)
- [IRS Publication 519](#) (Tax Guide for Aliens)

NIST REQUIRED FORMS

- [Visitor Registration Form](#)
- [NIST-1291](#), Foreign Guest Researcher Agreement
- [NIST-351, Request for Federal Credential or NIST Site Badge](#)
- Attachment 2 of [DAO 207-12](#) “Certification of Conditions and Responsibilities for Departmental Sponsors of Foreign National Guests”
- Attachment 3 of [DAO 207-12](#), “Certification of Conditions and Responsibilities for a Foreign National Guest”

CIRCUMSTANCE-SPECIFIC REQUIRED FORMS

- [IRS W8-BEN Form](#)
- [Form DN-45, Invention Disclosure and Rights Questionnaire](#)
- [Department of Commerce Foreign National Visitor and Guest Access Requirements Document](#)
- [NIST Form-1284, Access Change Request](#)

DEFINITIONS

Foreign Guest Researcher (FGR) - any technically qualified person who is not a U.S. citizen and is sponsored by an organization other than NIST, or is self-employed, or is working at NIST under the auspices of a NIST funding agreement (contract, grant, cooperative agreement, or simplified acquisition), and collaborates with NIST on research projects and/or technical activities of mutual interest. A FGR may be an employee of a foreign government agency; Federal, state, or local government agency; for-profit company; non-profit organization (including a college or university); or be a postgraduate researcher or graduate student; or be self-employed.

There are three types of FGRs defined in the NIST Associates Information System (NAIS):

1. Research and Science (FGRRS): This category includes those individuals who collaborate with NIST on research projects of mutual interest.
2. Technical (FGRTEC): This category includes those individuals who provide on-site technical computer services (e.g. programming, network or systems administration) or conduct market research, strategic planning, and/or other consulting services.
3. Special Programs (FGRSPL): This category includes technically qualified students who participate in the Summer Undergraduate Research Fellowships Program (SURF) or the Professional Research Experience Program (PREP), or as a Postdoc - Department of Homeland Security (PD-DHS), as a NIST/National Institutes of Health (NIH) National Research Council (NRC) Postdoc - National Institute of Health (PD-NIH) or on another NIST Fellowship Program.

REQUIREMENTS

- NIST shall make its facilities available for FGRs to pursue scientific or technical projects of mutual interest under conditions determined by NIST.
- A NIST 1291 (FGR Agreement) must be approved and signed by the FGR before the FGR uses NIST facilities and equipment, with or without IT access, to conduct research.
- A FGR may not perform the work of a NIST employee.
- A NIST project may not be solely dependent on a FGR's involvement.

- A FGR shall work collaboratively under the oversight of a designated NIST host.
- The length of stay of the FGR may be subject to availability of funds, visa status, equipment availability and/or appropriate laboratory facilities.
- A FGR may not participate in a Cooperative Research and Development Agreement (CRADA) or in other NIST activities involving proprietary information.

Processing

- The [NIST Associate Information System \(NAIS\)](#) process must be completed for all FGRs.
- For entry on the NIST Gaithersburg and Boulder sites, the host must enter the FGR into the NIST on-line visitor registration system prior to their arrival: This can be done through NAIS. For visits of three days or less, visitor registration must be completed 72 hours in advance. For visits of three days or more, visitor registration must be completed 30 days in advance.

Security

- A FGR must meet all NIST security requirements.
- Security investigations shall not be required if a FGR is at NIST for ten days or less. In compliance with the [U.S. Department of Commerce Manual of Security Policies and Procedures](#), such individuals must be escorted by a NIST employee at all times
- A FGR will not be issued a security badge, issued an information technology (IT) resource account, or provided with a NIST telephone extension without being processed through NAIS.
- Citizens of Countries designated as State Sponsors of Terrorism <http://www.state.gov/j/ct/list/c14151.htm> shall not be permitted as NIST FGRs unless they are Legal Permanent Residents (LPRs) of the United States. Please contact IAAO for guidance.
- The NIST host of a FGR shall follow the Department of Commerce security requirements listed in the Department Administrative Order (DAO) 207-12 “Foreign National Visitor and Guest Access Program.”
- The NIST host of a FGR shall attend the Espionage Indicators Training (also known as Counterintelligence Briefing) annually. The NIST Office of Security will present briefings throughout the year.
- Upon the FGR’s arrival, the NIST host shall complete Attachment 2 of [DAO 207-12](#) “Certification of Conditions and Responsibilities for Departmental Sponsors of Foreign National Guests” for each FGR sponsored, and forward it to the Emergency Services Division.

- Upon arrival, the NIST host shall have the FGR complete Attachment 3 of [DAO 207-12](#) “Certification of Conditions and Responsibilities for a Foreign National Guest,” and the NIST host shall forward it to the NIST Office of Security.

Financial Subsistence

- NIST may provide financial subsistence to defray the expenses of a FGR collaborating with a NIST employee on scientific or engineering research at NIST as per [Section 17 of the NIST Organic Act](#). NIST may only provide financial subsistence to FGRs on NIST sponsored J1 visas. This authority does not permit NIST to cover salary expenses. Federal tax is withheld at the rate of 14 percent for all NIST FGRs except those who are eligible for and claim the benefits of a tax treaty.
- A FGR wishing to claim the benefits of a tax treaty must complete an [IRS W8-BEN Form](#), and provide the completed form to the International and Academic Affairs Office (IAAO) prior to receiving tax treaty benefits. To assist in making the determination of tax treaty eligibility, FGRs will be provided with IRS [Publication 515](#) and [Publication 519](#) prior to arrival at NIST. A FGR who is working at NIST under a NIST funding agreement may not receive financial subsistence.
- Direct NIST subsistence payment to a FGR shall accrue against Scientific & Technical Research & Services (STRS) Project/Tasks.
- Financial subsistence may be amended in NAIS according to changing or unexpected conditions affecting the FGR’s tenure at NIST. All changes to financial subsistence payments are processed in NAIS and approved by Organizational Unit (OU) Director, IAAO Director, and the Finance Division.

Invention Disclosure

- The FGR shall disclose to NIST, using [Form DN-45, Invention Disclosure and Rights Questionnaire](#), any inventions made in the course of the project. Unless superseded by treaty, statute, or prior written agreement, NIST shall have the option to take the entire right, title, and interest in the United States to any such invention on behalf of the U.S. Government. NIST shall retain a non-exclusive, nontransferable, irrevocable, paid-up license to practice or to have practiced any such invention worldwide for or on behalf of the United States Government. Software and data prepared solely by NIST employees, prepared jointly by NIST employees and the FGR, or prepared solely by the FGR, shall not be copyrighted and shall be placed into public domain for unrestricted dissemination.

RESPONSIBILITIES

Host Division

- Assigns a host who is a NIST Employee;

- Adheres to the assignment and administrative procedures applicable to the NIST FGR Program;
- Defines or accepts the project and/or research objectives, the relevance of the scope to the mission of the host division, and work schedule of the FGR;
- Determines if FGR will have access to any export controlled information, determines if such access is consistent with [Export Control laws and regulations](#), ([5.21 Export Control](#)) and notates through the NAIS system accordingly;
- Determines if FGR will participate in research involving human subjects (see Directives [P 5500.00](#) and [O 5501.00](#)) and/or vertebrate animals ([14.02 Animal Care and Use](#)) and ensures that appropriate clearances for such research are obtained;
- Processes FGR paperwork in NAIS and appropriately classifies the FGR according to the intended scope of research and with consideration of the appropriate level of access to NIST assets and information;
- Provides safety orientation;
- Schedules IAAO entrance and exit briefings [at Boulder, the host division provides a general briefing upon arrival, collects information and submits to IAAO];
- Ensures all hosts and other division staff as deemed necessary attend the Espionage Indicators Training annually;
- For each FGR completes [DAO 207-12](#) (Attachment 2) and ensures FGR completes Attachment 3 of DAO 207-12;
- Informs the FGR of the obligation to conform to the usual administrative requirements and rules of conduct generally applicable to NIST employees, including protection of human and animal subjects and provides this information to the FGR;
- Obtains signature of the FGR on NIST-1291, Foreign Guest Researcher Agreement;
- Provides technical oversight to the FGR;
- Specifies type of IT Access in NAIS when needed; and
- If out of hours site access is requested, completes the Department of Commerce Foreign National Visitor and Guest Access Requirement document http://inet.nist.gov/ofpm/services/upload/FNV_AccessRequirements.pdf for approval by the Emergency Services Division and submits to the NIST Office of Security concurrently with the [NIST Form-1284, Access Change Request](#).
- Sponsors FGRs in US Access System for Personal Identity Verification (PIV) badge as appropriate (Boulder only).

Organizational Unit (OU)

- Reviews and approves NIST 1291, including description of research to be performed and proposed classification for suitability and eligibility, using the criteria defined in this Order.
- OU Director (or delegate) signs Form NIST-1291, Foreign Guest Researcher Agreement, as an approving official for NIST. This authority may be further delegated.

International and Academic Affairs Office

- Manages the NIST FGR Program;
- Reviews and negotiates modifications to Form NIST-1291, Foreign Guest Researcher Agreement, to ensure completeness and accuracy for approval;
- Maintains IRS Form W-8 BEN for FGRs claiming Tax Treaty Benefits;
- Reviews all financial subsistence to be provided to FGRs;
- Determines visa eligibility and provides administrative assistance to FGRs;
- Provides FGR a general entrance briefing upon arrival and an exit briefing prior to departure: For Gaithersburg, on-site briefing, for other locations, Video Teleconferencing (VTC) available upon request;
- Responds to inquiries concerning the NIST FGR Program;
- Prepares FGR program completion certificate prior to FGR's departure;
- Sponsors FGRs in US Access System for Personal Identity Verification (PIV) badge (Gaithersburg only); and
- IAAO Director (or delegate) signs Form NIST-1291, Foreign Guest Researcher Agreement, as an approving official for NIST. This authority may be further delegated.

NIST Office of Security (OSY)

- Reviews security investigation requests for completeness and accuracy and submits to the Office of Personnel Management;
- If requested, approves out-of-hours access once security investigation is complete;
- Maintains Attachment 3 of DAO 207-12 "Certification of Conditions and Responsibilities for a Foreign National Guest;" and
- Notifies the appropriate OUs regarding security investigation actions.

Emergency Services Division (ESD)

- Uses Form [NIST-351, Request for Federal Credential or NIST Site Badge](#), in NAIS to prepare and issue (for Gaithersburg), a site badge and PIV if appropriate. A site access

badge will be issued after the FGR submits the required security forms to the NIST Office of Security, completes the e-QIP (Electronic Questionnaire for Investigative Processing) process, and has been fingerprinted;

- Maintains Attachment 2 of DAO 207-12 “Certification of Conditions and Responsibilities for Departmental Sponsors of Foreign National Guests;” and
- If required, reviews and submits the Department of Commerce Foreign National Visitor and Guest Access Requirement form for Out of Hours access http://inet.nist.gov/ofpm/services/upload/FNV_AccessRequirements.pdf to the NIST Office of Security.

Boulder Badging Office

- Upon receipt of a DOC Boulder Laboratory Site Access Request Form and notification from the NIST Office of Security that all required security information (forms, completed e-QIP, and fingerprints) has been received, issues Boulder Access badge and PIV, if appropriate.

Finance Division

- Provides payment of financial subsistence to FGRs;
- Arranges electronic transfer of subsistence payments to an account at a U.S. financial institution of FGR’s choice;
- Withholds federal tax at the rate of 14 percent for all guest researchers not eligible to claim the benefits of a tax treaty; and reports to the Internal Revenue Service (IRS); and
- Provides [IRS Form 1042](#) annually to NIST FGRs receiving subsistence for tax preparation.

Office of Information Systems Management (OISM)

- Provides access to servers and maintains data files via the NIST Associates Information System (NAIS), if applicable; and
- Specifies type of IT access in NAIS when needed.

DIRECTIVE OWNER

109 - International and Academic Affairs Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	12/12/2012	Claire Saundry	Initial Draft
Rev. .01	12/14/2012	Dan Cipra	Removed the Procedure and created a new directive. Took care of some minor formatting changes as well.
Rev. .02	12/13/2012	Claire Saundry	Revised and sent to IAAO for comments
Rev. .03	12/14/12	Claire Saundry	Revised and sent to ESD, OSY and Finance for comments
Rev. .04	2/8/2013	IAAO office	Substantial Revisions – re-circulated to ESD, Finance, OSY
Rev. .05	2/19/2013	Claire Saundry	IAAO, ESD, OSY and Finance comments included. Revised text sent to M&O
Rev. .06	5/23/2014	Claire Saundry	Minor revisions to reflect changes in Boulder Security processing, re-reviewed by OSY
Rev. .07	2/27/2015	Dan Cipra	Accepted all OCC and IAAO comments and created a clean version.
Rev. .08	5/14/14	Claire Saundry	Revisions in response to DRB review
Rev. .09	5/19/15	Dan Cipra	Final changes based on DRB review.

Foreign Guest Researcher Program

NIST PR 1402.01
Effective Date: 5/26/2015

PURPOSE

This directive establishes NIST procedures for administrative processing and hosting of foreign guest researchers (FGRs), including use of the National Institute of Standards and Technology [Associates Information System \(NAIS\)](#), and defines responsibilities of various NIST offices involved. NIST PR 1402.01, together with NIST O 1402.00 replaces Administrative Manual Subchapter 5.14.

APPLICABILITY

The procedures outlined in this directive apply to all NIST employees involved with the administrative processing and hosting of Foreign Guest Researchers at NIST Gaithersburg, MD, NIST Boulder, CO, and Hollings Marine Laboratory, Charleston, SC.

REFERENCES

- NIST O 1402.00 Foreign Guest Researchers
- [IRS publication 515](#) (withholding Tax on Non-resident Aliens and Foreign Entities)
- [IRS Publication 519](#) (Tax Guide for Aliens)

REQUIRED FORMS

- [Visitor Registration Form](#)
- [NIST-1291](#), Foreign Guest Researcher Agreement (Must be completed within the [NAIS system](#)).
- [NIST-351, Request for Federal Credential or NIST Site Badge](#)
- Attachment 2 of [DAO 207-12](#) “Certification of Conditions and Responsibilities for Departmental Sponsors of Foreign National Guests”
- Attachment 3 of [DAO 207-12](#), “Certification of Conditions and Responsibilities for a Foreign National Guest”

CIRCUMSTANCE-SPECIFIC REQUIRED FORMS

- [IRS W8-BEN Form](#)

- [Form DN-45, Invention Disclosure and Rights Questionnaire](#)
- [Department of Commerce Foreign National Visitor and Guest Access Requirements Form](#)
- [NIST Form-1284, Access Change Request](#)
- [Verification of English Language Proficiency form](#)

PROCEDURES

I. Pre-Arrival of Foreign Guest Researcher (FGR)

- For a FGR coming from outside the United States, the International and Academic Affairs Office (IAAO) must receive the completed NAIS agreement process at least ***three*** months prior to scheduled arrival to NIST. If FGR is currently in the United States, and NIST is not the visa sponsor, IAAO must receive the completed NAIS agreement process at least 30 days in advance. Contact IAAO for guidance.
- Host division is responsible for data collection (forms and templates are available at: <https://inet.nist.gov/tpo/services/nais>) from the potential FGR and entering information into the NAIS system. NAIS will automatically generate required forms necessary to process a FGR agreement through IAAO, NIST Office of Security (OSY) and Finance Division (if applicable).
- Instructions on the NAIS system, including templates and checklists may be found at: <https://inet.nist.gov/tpo/services/nais-templates-and-forms>
- Host Division is responsible for documenting English Language Proficiency for potential FGRs on a NIST-sponsored J1 visa:
 - Guidance on Language Proficiency - <https://inet.nist.gov/sites/default/files/ELPT2015.pdf>
 - Verification of English Language Proficiency - <https://inet.nist.gov/sites/default/files/VELP2015.pdf>
- Host Division is responsible for identifying appropriate workspace, preparing desk and computer setup if applicable.
- Using NAIS, Host division:
 1. Determines length of FGR agreement;
 2. Develops research plan and description of the research to be accomplished, or for FGRs on NIST funding agreement, accepts the work plan of the contract, grant, cooperative agreement or simplified acquisition;

3. If applicable, determines financial subsistence, airfare payment (airfare payment must be verified through NIST travel office to be within U.S. government rate) and any support to defray the costs of conference related expenses;
4. If under a NIST funding agreement (contract, grant, cooperative agreement or simplified acquisition), enters agreement type and number into NAIS and sends a copy of the funding agreement to IAAO either electronically as a supporting document attached to the NAIS process, or as a hard copy;
5. Determines the need for out-of-hours access and, if so completes [Department of Commerce Foreign National Visitor and Guest Access Requirements Document](#) and [NIST Form-1284, Access Change Request](#);
6. Submits all appropriate forms through NAIS for approval; and
7. Identifies in NAIS when Information Technology account is needed;
8. Assigns a NIST Employee buddy to be an escort for the guest researcher until he/she has been issued a NIST Site Badge.
9. Security Investigation Requirements:
 - If the length of stay is ten working days or less, a security investigation is not required. In NAIS, select the security opt-out process. These FGRs must be escorted on the NIST site by a NIST Employee buddy at all times.
 - If the length of stay is greater than ten working days, the security opt-out process may not be selected. NAIS will generate all required security forms for processing.
 - For visits greater than 180 days, once the NAIS process is complete, including the appropriate selection of classification and clearance, OSY emails FGR an invitation to the Electronic Questionnaires for Investigations Processing (e-QIP) system.
 - For each FGR sponsored, regardless of duration of appointment, the NIST host is required to complete Attachment 2 of Department Administrative Order (DAO) 207-12 [“Certification of Conditions and Responsibilities for the Departmental Sponsor of Foreign National Guests”](#) and submit completed paperwork to the NIST Emergency Services Division (ESD).
 - All NIST hosts who sponsor FGRs are required to complete the Espionage Indicators Training (also known as Counterintelligence Briefing) annually. NIST OSY is responsible for scheduling and presenting briefings.
 - For FGR’s entry to NIST, the host division is responsible submitting FGR’s information, though NAIS into the NIST on-line visitor registration system

prior to scheduled arrival date (30 days in advance for visits of more than 3 days, and 72 hours in advance of visits 3 days or less).

- Unescorted out-of-hours access to the NIST campus is contingent upon satisfactory completion of the security investigation and an approved [DOC OSY Access Request document](#). The host division initiates an update process in NAIS and changes the requested access level for out-of-hours approval.
- Potential FGRs that are citizens of countries designated as State Sponsors of Terrorism, must be Legal Permanent Residents (LPRs) of the U.S. to be eligible to be a NIST FGR. The NIST OSY maintains a list of these countries.

II. Foreign Guest Researcher Agreement Approval Process:

- The NAIS process is initiated by the Host Division, sent to Organizational Unit (OU) Director (or designee) for approval, forwarded to IAAO for approval and to Finance Division for approval if appropriate.
- IAAO reviews FGR agreement for accuracy and collects all necessary supporting documents, which include passport, visa and funding agreement information for final approval. If no financial subsistence is requested, IAAO is the final step in approving the NAIS agreement.
- The NIST Finance Division reviews the subsistence portion of the agreement for accuracy and verifies Project/Task, payment dates and fiscal year information.
- If receiving NIST financial subsistence, FGRs are subject to 14 percent withholding unless claiming the benefit of a tax treaty.
 - To claim a tax treaty benefit, a FGR must have a valid social security number and a completed [IRS W8-BEN Form](#) (time sensitive action) on file in IAAO. IRS publications 515 (www.irs.gov/publications/p515/index.html) and 519 (<http://www.irs.gov/pub/irs-pdf/p519.pdf>) are provided to assist FGR in making the determination of tax treaty eligibility.
- If a FGR has a valid U.S. social security number and the IRS W8-Ben form is returned to IAAO at least one month prior to scheduled arrival at NIST, tax will not be withheld from subsistence payments. If the IRS W8-BEN form is not submitted to IAAO, 14 percent will be deducted automatically from monthly subsistence payments until a valid social security number and IRS W-8 BEN form have been submitted.
- IAAO is responsible for preparing J1 (DS-2019) visa forms and providing pertinent information concerning NIST's J1 Visa Program. Once the J1 visa information package is complete:

- For NIST Gaithersburg and Hollings Marine Laboratory in Charleston: IAAO emails host/initiator with information on pick up and shipment procedures.
- For Boulder: IAAO mails entire J1 visa information package with shipment instructions, along with arrival instructions to Boulder host/initiator.

III. Arrival of Foreign Guest Researcher:

Host division:

1. Enters actual arrival date into NAIS;
2. Ensures the FGR completes Attachment 3 of DAO 207-12 “Certification of Conditions and Responsibilities for a Foreign National Guest” and forwards to OSY in Gaithersburg within 72 hours of arrival;
3. If IT resources are requested, ensures FGR has read and signed the NIST Policy on Information Technology Resources Access and Use http://inet.nist.gov/oism/directives/iss_aup.cfm; takes IT security orientation; obtains IT account; and participates in IT security training as provided by OISM;
4. Follows OU-established policies and procedures regarding the safety training of new employees/associates. Go to <http://safety.nist.gov> for the required safety training;
5. For Gaithersburg, completes security forms, e-QIP, and schedules an appointment with OSY on day of arrival;
6. Obtains the FGR’s signature on form NIST-1291, Foreign Guest Researcher Agreement, enters signature date into NAIS, which notifies OSY that the process is complete; submits signed NIST 1291 electronically through NAIS;
7. For NIST Gaithersburg: schedules entrance appointments with IAAO;
8. For NIST Boulder: Provides entrance briefings, provides NIST Boulder specific policies and procedures; prints and submits required security package forms and fingerprints to OSY, and collects and submits information to IAAO;
9. For NIST Boulder: If prompted by NAIS, sponsors the FGR to receive a Personal Identification Verification (PIV) card in the U.S. Access System and explains the PIV process to the FGR;
10. Prepares appropriate NAIS financial updates for changes in subsistence payments resulting from delayed arrival, early departure, or changing subsistence needs;

11. FGR is responsible for submitting the completed e-QIP forms to OSY within 3 working days of arrival;
12. For FGRs receiving subsistence, the first check is issued by the NIST Finance Division and must be picked up on the last workday of the month prior to FGR's arrival month by Host Division;
 - i. For NIST Gaithersburg: Check pickup in Administration Building 101, Room A800 Accounts Receivable Office between 1:00pm-3:00pm by authorized NIST personnel only.
 - ii. For NIST Boulder: Finance Division sends checks to the EMSS/Boulder Maintenance and Support Services Division for pick-up by authorized NIST personnel.
 - iii. For Hollings Marine Laboratory: Check pickup, by an authorized NIST staff member at NIST Gaithersburg in Building 101, Room A800 between 1:00pm-3:00pm, then mailed to FGR by host division.
13. Once a security investigation has been completed, after-hours access may be requested. To request after-hours access, host division submits the following:
 - a. For Gaithersburg: the Department of Commerce Foreign National Visitor and Guest Access Requirement Document (ARD)http://inet.nist.gov/ofpm/services/upload/FNV_Access_Requirements.pdf) and NIST 1284 through NAIS. ARD is sent to ESD for review and submission to NIST OSY. Once approved after-hours access may be granted.
 - b. For Boulder: submits the Department of Commerce Foreign National Visitor and Guest Access Requirement Document http://inet.nist.gov/ofpm/services/upload/FNV_Access_Requirements.pdf) through the Boulder Laboratory Operations Director (BLOD) for review; BLOD office submits to ESD for review and submission to NIST OSY. Once approved after-hours access may be granted by the EMS office in Boulder

IAAO:

1. At Gaithersburg, provides on-site entrance briefing for FGRs with general information on NIST's policies and procedures; for other locations, VTC is available on request;
2. If NIST is the visa sponsor, provides information on NIST's J1 Exchange Visitor Visa Program;

3. Provides each FGR with information on health insurance requirements and collects certification that FGR has appropriate health insurance;
4. If a FGR claims a tax treaty benefit and possesses a social security number, collects the completed IRS W8-BEN form and enters information into NAIS to stop tax withholding;
5. Provides FGRs with information on obtaining a Social Security number and instructions to inform the NIST Finance Division once the number is received;
6. Provides information on opening a bank account, along with appropriate form for the NIST Finance Division to arrange electronic transfers of monthly subsistence payments;
7. If prompted by NAIS, sponsors the FGR to receive a Personal Identification Verification (PIV) card in the U.S. Access System and explains the PIV process to the FGR.

OSY:

1. For Gaithersburg: OSY meets with the FGR and ensures all security forms, completed e-QIP, and fingerprints have been submitted. Upon completion of security requirements, a site badge may be issued.
2. For Boulder: OSY asserts that all security forms, completed e-QIP and fingerprints have been submitted and sends the Boulder Badge Office notification for FGR to be issued site access badge.
3. Reviews and approves out of hours access requests.

Emergency Services Division (ESD):

1. Upon receipt of a NAIS generated form NIST-351, prepares and issues a site access badge.
2. Upon receipt of required documentation, prepares and issues a PIV badge, as appropriate.
3. Reviews and approves NIST-1284 and the Department of Commerce Foreign National Visitor and Guest Access Requirement document in NAIS and submits to NIST OSY.

Boulder Laboratory Operations Director (BLOD):

1. Reviews ARD request for out of hour access and submits to ESD for review and submission to NIST OSY.

Emergency Management Services Office, Boulder:

1. Once approved by BLOD, ESD and OSY may granted out of hours access to NIST Boulder site.

IV. Departure Procedures for Foreign Guest Researcher:

- The host division is responsible for entering actual departure date in NAIS on date of departure.
- Departure checklists are available at: <https://inet.nist.gov/tpo/services/nais-templates-and-forms>
- The host division is responsible for ensuring that FGR is removed from telephone directory; and all library books, keys and badge are returned, and property system is updated as necessary.
- If a FGR is on NIST sponsored J1 visa, the host division is responsible for providing at least three days advance notice to IAAO of departure date.
- Upon notification of departure from NIST Gaithersburg, IAAO will contact the FGR to schedule an exit briefing and present the completion certificate, collect a forwarding address, and answer any questions.
- The host division is responsible for preparing form NIST-1251, Hazardous Materials Clearance for Nonemployees, if applicable.
- For additional assistance in FGR departure procedures, please refer to the NAIS generated NIST Associate Separation Clearance Worksheet:
<https://inet.nist.gov/tpo/services/nais-templates-and-forms>

V. Extension of a Foreign Guest Researcher Agreement:

- The host division is responsible for preparing a NAIS agreement extension. Using NAIS, the host division prepares and submits through the OU a new form NIST-1291, marking the “Agreement” block as an extension. The host division forwards the form through the NAIS approval process.

- IAAO notifies FGR/host/initiator that agreement extension is complete.

For NIST Gaithersburg: IAAO schedules appointment for FGR to sign the agreement extension (if applicable, sign updated visa (DS2019) form). IAAO enters the signature date into NAIS. IAAO prompts the FGR to schedule an appointment with OSY to renew their NIST badge.

For NIST Boulder and Hollings Marine Laboratory: IAAO instructs the host/initiator to obtain the FGR’s signature on the form NIST-1291 and collect and

send all other pertinent information to IAAO. Once the form NIST-1291 and other supporting documents are returned to IAAO, IAAO enters the signature date into NAIS, which releases security information to OSY.

VII. Cancellation of Foreign Guest Researcher Agreement

- The host division is responsible for cancelling the FGR agreement in NAIS. NAIS automatically notifies the appropriate NIST offices.

DIRECTIVE OWNER

109 - International and Academic Affairs Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	12/12/2012	Claire Saundry	Initial Draft
Rev. 0.01	12/12/2012	Dan Cipra	Formatting changes only
Rev. 0.02	12/13/2012	Claire Saundry	Revised and sent to IAAO for comments
Rev. 0.03	12/14/12	Claire Saundry	Revised and sent to ESD, OSY and Finance for comments
Rev. 0.04	2/8/2013	IAAO office	Substantial Revisions – re-circulated to ESD, Finance, OSY
Rev. 0.05	2/19/2013	Claire Saundry	IAAO, ESD, OSY and Finance comments included. Revised text sent to M&O
Rev. 0.06	5/23/2014	Claire Saundry	OSY review and minor edits to Boulder Security due to changes since previous OSY review.
Rev. 0.07	2/27/2015	Dan Cipra	Created clean copy with OCC and IAAO changes
Rev. 0.08	5/14/15	Claire Saundry	Revised to address DRB comments
Rev. 0.09	5/19/15	Dan Cipra	Incorporated all DRB Comments

New Category of Foreign Guest Researcher

NIST N 1402.01
Effective Date: 8/5/2016

PURPOSE

The purpose of this notice is to create the new category of National Institute of Standards and Technology (NIST) Foreign Guest Researcher (FGR), under the existing heading of FGR Special Programs (FGRSPL), for participation in research collaborations and training workshops lasting 10 business days or less. For this new category only, NIST will allow a modest stipend to be provided to an FGR on a B1 Business visa.

APPLICABILITY

This notice applies to all NIST employees involved with the administrative processing and hosting of Foreign Guest Researchers at NIST for stays of 10 business days or less to participate in short-term research collaborations or training workshops.

REFERENCES

- NIST P 1400 [Visiting Researcher and Associate Policy](#)
- NIST O 1402.00 [Foreign Guest Researcher Program](#)
- NIST PR 1402.01 [Foreign Guest Researcher Program Procedures](#)
- NIST PR 1400.01 [Foreign Visitors](#)
- [U.S. Citizenship and Immigration Services information on B-1 Temporary Business Visitor travel to the United States](#)
- [U.S. Department of State information on Business travel to the United States](#)
- [NIST FGR Monthly Subsistence Limit](#)

BACKGROUND

The NIST FGR Program, a key mechanism by which NIST engages with our foreign counterparts, enables our laboratories to host talented scientists with skills that provide our staff with new insights, perspectives, and expertise.

However, current protocols for hosting FGRs do not provide adequate flexibility for short-term collaborative activities or training workshops. While the FGR Program is the means by which NIST sponsors medium-to long-term stays by researchers on J1 visas, there is also a need for a separate category of NIST FGR to enable short-term collaborations and training at less cost to both NIST and the exchange visitor's institute.

Please see the February 19, 2016 Memo (Appendix A) from the Associate Director for Laboratory Programs (ADLP) regarding a new NAIS category to support and facilitate short-term technical exchanges.

DEFINITIONS

Short-Term – 10 business days or less

FGRSPL TRG/WSHP – Foreign Guest Researcher Special Programs Training/Workshop.

REQUIREMENTS

- A new type of associate called the Foreign Guest Researcher Special Programs Training/Workshop (FGRSPL TRG/WSHP) shall be created
- Research collaborations and training under the FGRSPL TRG/WSHP shall be 10 business days or less
- A B1 Business visa will be acceptable to NIST for participation as an FGRSPL TRG/WSHP
- The FGRSPL TRG/WSHP shall include the ability to provide a stipend
- Revise NIST O 1402.00 and NIST PR 1402.01 to incorporate the change

DIRECTIVE OWNER

109 – International and Academic Affairs Office

APPENDICES

A - February 19 2016 Memo from the Associate Director for Laboratory Programs (ADLP)

B - Revision History

APPENDIX A

FEBRUARY 19 2016 MEMO FROM THE ASSOCIATE DIRECTOR FOR LABORATORY PROGRAMS (ADLP)

FEB 19 2016



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

MEMORANDUM FOR: Kevin Kimball
Chief of Staff

FROM: Kent Rochford *KBR*
Associate Director for Laboratory Programs

SUBJECT: NAIS category to support and facilitate short-term technical exchanges

The National Institute of Standards and Technology (NIST) plays an important role in the advancement of measurement science throughout the world. Engaging our international counterpart organizations in ways that compliment our own research priorities allows NIST to promote the interests of U.S. industry and develop partnerships that result in mutually beneficial gains. Collaborations between NIST researchers and their scientific peers abroad have helped to further and enhance the products and services we provide to our customers and stakeholders.

The NIST Foreign Guest Researcher (FGR) Program, a key mechanism by which NIST engages with our foreign counterparts, enables our laboratories to host talented scientists with skills that provide our staff with new insights, perspectives and expertise. In addition to this, those foreign researchers who collaborate with our staff return to their respective organizations with an improved understanding of metrology and often take up leadership positions within their own National Metrology Institutes. The NIST FGR Program reinforces the strategic partnerships we have with other prominent members of the international science and technology community.

It has come to the attention of NIST's leadership that the current protocols surrounding the acceptance of FGR Program do not provide adequate flexibility for particular collaborative training endeavors. While the FGR Program should and will remain the means by which NIST sponsors medium- to long-term stays by researchers on J1 visas, NIST management recognizes the need for a separate category of NIST FGR to enable short-term collaborations and training requiring less financial burden on both NIST and the exchange visitor's respective institute.

It is for these reasons I am instructing the International and Academic Affairs Office (IAAO) to create a new NIST FGR category for research collaborations and training lasting 10 days or less under the existing heading of FGR Special Programs (FGRSPL). For this new category only, in an effort to lower obstacles to collaborative training activities, NIST will allow use of a B1 Business visa for stays of 10 days or less, and the ability to provide a stipend for this category of FGR. All other rules and requirement in place for FGRs hosted by NIST will remain in place. I further instruct IAAO to revise the relevant NIST Directives (NIST O 1402.00 and NIST PR 1402.01) to address this change.

cc: IAAO – C. Saundry

NIST

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	18 Apr 2016	Claire Saundry (IAAO)	Draft
Rev. .01	25 Apr 2016	Dan Cipra (M&O)	Formatting
Rev. 02	16 May 2016	Claire Saundry (IAAO)	Corrected date of Memo

Letters to Support Petitions for United States Legal Permanent Residency

NIST O 1403.00
Effective Date: 4/28/2016

PURPOSE

This Order describes the requirements and responsibilities for review and approval of an official National Institute of Standards and Technology (NIST) reference letter written in support of an application for United States (U.S.) Legal Permanent Resident (LPR) status by a Foreign NIST Associate (FNA) with whom NIST has had a long-term, direct, professional working relationship.

APPLICABILITY

This Order applies to official communications, prepared by a NIST Federal employee to the Bureau of Citizenship and Immigration Services of the Department of Homeland Security, in support of an application for U.S. LPR status by an FNA with whom NIST has had a long-term, professional working relationship based on direct interactions.

This Order does not apply to requests from the general public for an official NIST letter in support of an application for U.S. LPR status.

This Order does not apply to a Foreign National (FN) NIST is recruiting for employment who is covered by NIST O 3112.00 and NIST PR 3112.01.

REFERENCES

- [J1 Visa Exchange Visitor Program](#)
- [National Interest Waiver](#)
- [NIST P 1400.00 Visiting Researcher and Associate Policy](#)
- [NIST O 3112.00 Employment of Non-U.S. Citizens Order](#)
- [NIST PR 3112.01 Employment of Non-U.S. Citizens Procedure](#)
- [Bureau of Immigration and Citizen Services](#)

BACKGROUND

Scientific progress relies on access to qualified technical experts to foster the open exchange of ideas, information, and results. NIST Federal employees work with visiting researchers and leading experts from all over the world, and NIST benefits from the ability to attract the best and brightest to work in the NIST laboratories. In some cases, an FNA seeking U.S. LPR status

requests a letter of support from NIST. Because of our specialized knowledge of the FNA, NIST's judgement is highly valued. However, as an agency of the Federal government and in the interest of maintaining NIST's reputation for high-quality work product, communications that indicate NIST support of an application for U.S. LPR status must be reviewed, as delineated below, prior to those communications occurring.

NIST participates in the J1 Exchange Visitor Program, and has the authority to sponsor J1 visas for FNAs participating in collaborative research activities at NIST. The purpose of the J1 Exchange Visitor Program is to foster global understanding through educational and cultural exchanges. All exchange visitors are expected to return to their home country upon completion of their program in order to share their exchange experiences. Therefore, a letter of support may not be provided to a FNA on a NIST-sponsored J1 visa.

REQUIREMENTS

- Letters may only be provided for an FNA with whom NIST has had a long-term, professional working relationship based on direct interactions, and only if the individual's continued presence in the U.S. directly supports a NIST program
- Letters must be written on NIST letterhead and signed by a NIST Federal employee who has professional knowledge based on direct interactions with the individual
- Letters must document the writer's qualifications to issue the letter
- Letters must document the writer's knowledge of the FNA's work, background, and achievements
- Letters must document the FNA's contributions to the field, evidence the FNA's international recognition and note the on-going and future value to NIST programs
- Letters must demonstrate U.S. national interest and impact on scientific field as a whole
- Letters must factually demonstrate how departure of the FNA would adversely impact NIST programs
- Letters must be reviewed and approved by the Office of the Chief Counsel (OCC) for NIST for legal requirements
- Letters must be reviewed and approved by the International and Academic Affairs Office (IAAO) to ensure FNA is not on a NIST-sponsored J1 visa
- A decision memo, reviewed and approved by the author's supervisor, Division Chief (or equivalent), Organizational Unit (OU) Director, OCC, and IAAO must accompany the letter to the appropriate Associate Director (AD) or designee for approval to ensure compliance with NIST policy

- In cases where an author is not organizationally located within a Division, Office, or Center, the author's supervisor fills the role of Division Chief or Office or Center Director

RESPONSIBILITIES

The NIST Director

- Review and approve the letter of support prior to communication
- Delegates this responsibility to the appropriate NIST AD, who may further delegate

Organizational Unit (OU) Directors

- Establish OU requirements for reviews and approvals that are delegated
- If so delegated by the appropriate NIST AD, may provide final review and approval

OU Directors (in addition to the responsibilities outlined above), Subordinate Managers (e.g. Division Chiefs (or equivalent), Office Directors, Center Director), and Other Supervisors (e.g. Group Leaders, Program Managers)

- Ensure compliance with this Order by NIST Federal employees performing technical activities under their direction
- Assure the editorial quality of letters prepared by NIST Federal employees who report to them
- Approve communications prepared under their supervision based on a determination that FNA's presence in the U.S. directly supports a NIST program
- Identify issues that may require additional levels of review

Authors of Letters

- Prepare letters (this task may not be delegated) that are of high quality, technically accurate, and editorially correct
- Identify issues that may require additional levels of review

Office of the Chief Counsel for NIST

- Assure letters meet legal requirements

Office of International and Academic Affairs

- Ensure the FNA is not on a NIST sponsored J1 visa
- Approve communications written in support of any FNA

DIRECTIVE OWNER

109 – International and Academic Affairs

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	2/10/2016	Claire Saundry	Initial draft
Rev. .01	2/16/2017	Claire Saundry	Comments received from James Olthoff, Ron Boisvert, Jon Pratt, and Nate Newbury
Rev. .02	2/18/2016	Dan Cipra	Formatting updates only
Rev. 03	4/5/2016	Claire Saundry	Revised to address DRB comments

Research Library, Publishing, and Museum Services

NIST P 1500.00
Effective Date: 9/8/2015

PURPOSE

This directive establishes the governing policy for the provision of library, publishing, and museum services by the Information Services Office (ISO).

SCOPE

For library and museum services, this policy applies to all NIST Gaithersburg employees and Associates engaged in research activities at NIST Gaithersburg, to the extent allowed by law and the terms of the Associate's agreement. Publishing services covered by this directive apply to all NIST employees and all Associates engaged in research activities at or for NIST, to the extent allowed by law and the terms of the Associate's agreement.

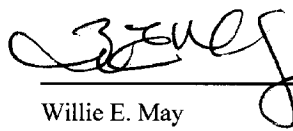
LEGAL AUTHORITIES AND REFERENCES

- Public Law 100-519, Section 107 (Oct 24, 1988)
- NIST O 5701.00, Managing Public Access to Results of Federally Funded Research, 6/26/2015
- Administrative Manual Subchapter 4.09, Technical Communications Program

POLICY

In accordance with law, NIST maintains a research information center to support the research, publishing, and preservation needs required to fulfill the scientific and technical mission of NIST. This includes acquiring, organizing, and making accessible print and digital information resources germane to the programs and research at NIST; publishing the NIST Technical Series and creating, curating, and maintaining metadata for published articles, technical series publications, and NIST research data in support of Managing Public Access to Results of Federally Funded Research; and acquiring, preserving, and displaying artifacts and archival materials that serve as a portion of the scientific record of NIST's achievements and history.

The Director ISO is responsible for defining and developing requirements and operational procedures that direct and guide the delivery of services. The ISO Director ensures that service quality is maintained through regular communication with stakeholders and customers, including the Research Library Board.



9/8/15

Willie E. May
Director

Date

NIST Research Library Services

NIST O 1501.00
Effective Date: 9/17/2015

PURPOSE

This directive establishes the requirements for the provision and use of library services at NIST Gaithersburg. This directive replaces Administrative Manual Subchapter 5.02.

APPLICABILITY

This order applies to all NIST Gaithersburg employees and Associates engaged in research activities at NIST Gaithersburg, to the extent allowed by law and the terms of the Associate's agreement.

LEGAL AUTHORITIES AND REFERENCES

- [Public Law 100-519, Section 107 \(Oct 24, 1988\)](#)
- [U.S. Code Title 17, Section 108 \(Copyright – Reproduction by libraries and archives\)](#)
- [NIST P 1500.00 NIST Research Library, Publishing, and Museum Services \(9/8/15\)](#)
- [NIST O 3115.00 Separation Clearance \(9/12/09\)](#)
- [NIST PR 1402.01 Foreign Guest Researcher Program Procedures \(5/28/15\)](#)

DEFINITIONS

- E-devices: mobile devices that contain e-books and other library resources that are available for borrowing from the Research Library.
- Information Resources: books, journals, and databases, regardless of their format (e.g., print, electronic).

REQUIREMENTS

The Information Services Office (ISO) will:

- Select, acquire, organize, and maintain print and digital information resources required to support the programs, research, and mission of NIST for use by all employees and Associates engaged in research activities at or for NIST Gaithersburg, to the extent allowed by law and the terms of the Associate's agreement in the physical library, at their desktop or hand-held e-device, or through remote access when off campus.
- Manage the access to library information resources whether received by purchase, license, or gift.

- Establish and carry out lending and use procedures for information resources in the Research Library's print and digital collections for loans to all employees and Associates engaged in research activities at or for NIST Gaithersburg to the extent allowed by law and the terms of the Associate's agreement.
- Retain an archival collection (in print and digital formats) of NBS/NIST Technical Series publications and historical information (e.g., photographs, oral histories).
- Establish and carry out procedures for use of the Research Library collections by the general public.

RESPONSIBILITIES

Director, Information Services Office

- Selects the information resources to be acquired or withdrawn from the library's collections, with assistance from the Research Library staff.
- Ensures all acquired or licensed information resources are processed to indicate NIST ownership or licensed to NIST.
- Determines lending and use procedures of the Research Library collections, e-devices, and equipment.

NIST Gaithersburg employees and Associates who borrow and use the Research Library's information resources and e-devices are responsible for:

- Complying with the Research Library's lending and use procedures for (a) loan periods, (b) renewals, (c) recalls, (d) lost items, and (e) clearance upon separation from NIST.

DIRECTIVE OWNER

135 – Information Services Office, Management Resources

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Release	12/14/14	Barbara Silcox	
Rev 1	12/15/14	Barbara Silcox	Incorporated comments from internal reviewers
Rev 2	1/15/15	Barbara Silcox	Incorporated comments from reviewers (stakeholders & customers)
Rev 3	7/8/15	Barbara Silcox	Incorporated comments from OCC
Rev 4	8/14/15	Barbara Silcox	Incorporated comments from DRB

Procedures for Borrowing Information Resources and E-Devices from the NIST Research Library

NIST PR 1501.01
Effective Date: 9/15/2015

PURPOSE

This directive establishes the procedures and responsibilities for borrowing information resources and e-devices from the NIST Research Library (Gaithersburg).

APPLICABILITY

The procedures apply to all NIST employees and Associates engaged in research activities at NIST Gaithersburg, to the extent allowed by law and the terms of the Associate's agreement.

REFERENCES

- [O 1501.00 NIST Research Library Services \(9/17/2015\)](#)

DEFINITIONS

- E-devices: mobile devices that contain e-books and other library resources that are available for borrowing from the Research Library.
- Information Resources: books, journals, and databases, regardless of their format (e.g., print, electronic).

RESPONSIBILITIES

Director, Information Services Office

- Determines lending and use guidelines and procedures of the Research Library that cover the types of materials and information resources that may be borrowed from the Research Library; the loan and renewal periods; and how overdue and lost items will be handled.

NIST Gaithersburg Employees

- May borrow information resources and e-devices from the Research Library with their NIST Federal PIV badge according to the procedures and loan periods set by the Research Library.
- Must return all borrowed items recalled by the Research Library or when separating from NIST. (See [Order 3115.00 Separation Clearance \(9/12/09\)](#) and [Form CD-126](#), Separation Clearance Certificate Supplemental Sheet).

- Must replace or pay replacement costs for any lost or damaged item borrowed from the Research Library.

NIST Associates - Gaithersburg

- All NIST Associates who have a NIST Federal PIV badge and a NIST IT Account, as verified in the NIST Identity and Access Management System (IDAM), may borrow information resources and e-devices from the Research Library.
- Must follow the Research Library's procedures for borrowing information resources and e-devices, including returning all borrowed items recalled by the Research Library or when separating from NIST.

NIST Gaithersburg Hosts/Sponsors

- Must ensure that items borrowed from the Research Library by Associates they host/sponsor are returned to the Library upon the Associate's separation from NIST. ([See Associate Separation Clearance Worksheet](#))

PROCEDURES

- Research Library users may borrow items from the Research Library's collection by charging them out at the Information Desk in the library using a valid NIST ID badge. Information on loan periods, renewals, and recalls is posted to the [NIST Virtual Library \(NVL\)](#).
- Research Library account status notices are electronically generated monthly and sent to borrowers and Host/Sponsors of NIST Associates to inform them of due dates.
- Research Library account status notices are sent to Hosts/Sponsors of Associates five weeks prior to the Associate's badge expiration date.
- Research Library users should inform Library staff when items are lost, stolen, or destroyed. Research Library users who do not replace or pay for these items will lose their borrowing privileges.
 - Research Library staff will advise the user of the cost of the replacement, based on the price listed in a current publisher or book vendor catalog.
- To borrow e-devices, Research Library users must come to the Research Library and sign an e-reader responsibility agreement and a 30-day property loan slip.
- The Research Library staff will obtain information resources from other libraries and other suppliers when they are not available in the NIST Research Library.
 - Research Library users must abide by the lending organization's loan period for items borrowed from other libraries on their behalf. Specific information on how to request items through the Research Library's Interlibrary Loan service can be found on the [NIST Virtual Library \(NVL\)](#).

- The lending library determines the cost of replacing a lost or damaged item; the employee or the Associate's division will be responsible for covering this cost. Once the lending library has communicated the procedure for replacing or covering the cost of the item, the employee's or Associate's interlibrary loan and document delivery privileges will be blocked until the lending library confirms that its conditions have been met.
- Prior to separating from NIST, Research Library users must return all borrowed items to the Research Library and make payment on any outstanding costs for borrowed items.

DIRECTIVE OWNER

135 - Information Services Office, MR

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Release	12/14/14	Barbara Silcox	
Rev 1	12/15/14	Barbara Silcox	Incorporated comments from internal reviewers
Rev 2	1/15/15	Barbara Silcox	Incorporated comments from reviewers (stakeholders & customers)
Rev 3	7/8/15	Barbara Silcox	Incorporated comments from OCC
Rev 4	8/14/15	Barbara Silcox	Incorporated comments from DRB

Publishing Services – NIST Technical Series Publications and the *Journal of Research of the National Institute of Standards and Technology*

NIST O 1502.00
Effective Date: 6/7/2016

PURPOSE

This directive establishes the requirements and associated roles and responsibilities for the dissemination, preservation, and management of NIST Technical Series publications, including the *Journal of Research of the National Institute of Standards and Technology*. This directive replaces Administrative Manual Subchapter 4.09 Appendix K and section 4.09.06g.

APPLICABILITY

This Order applies to:

- All NIST employees, including full- and part-time employees, temporary government employees, and special government employees, who publish scholarly and technical material as part of their employment.
- All NIST associates engaged in research activities at or for NIST who publish scholarly and technical material to the extent allowed by law and the terms of the associate's agreement.

REFERENCES

- [DAO 201-1 Approval and Use of Seals, Emblems, Insignia, and Logos](#)
- [DAO 201-17 Seal of the Department of Commerce](#)
- [DAO 205-1 Records Management](#)
- [DAO 219-1 Public Communications](#)
- [NIST P 1500.00 NIST Research Library, Publishing, and Museum Services](#)
- NIST O 1801.00 Review of Technical Communications
- [NIST O 5701.00 Managing Public Access to Results of Federally Funded Research](#)
- [NIST Comprehensive Records Schedule N1-167-92-1](#)
- [ANSI/NISO Z39.18-2005 \(R2010\) Scientific and Technical Reports - Preparation, Presentation, and Preservation](#)

DEFINITIONS

- Digital Object Identifier (DOI): A string of characters used to identify an object such as an electronic document.
- Federal Digital System (FDSys): A system operated by the U.S. Government Publishing Office (GPO) that serves as NIST's repository for NIST Technical Series publications, as well as other papers that have not been reviewed through an external publisher's peer-review process (e.g., conference proceedings, reports).
- NIST Technical Series – Publications published by or for NIST, intended for internal and external distribution. Descriptions are provided on the [NIST Virtual Library \(NVL\)](#).
- PubMed Central (PMC): [PubMed Central](#), maintained by the National Institutes of Health, which serves as NIST's repository for peer-reviewed publications, including the *Journal of Research of NIST*.

REQUIREMENTS

- Requirements for review and approval of manuscripts slated for publication in a NIST Technical Series, including the *Journal of Research of NIST*, are stated in NIST O 1801.
- Technical Series Publications shall:
 - bear the appropriate Department of Commerce (DoC) and National Institute of Standards and Technology (NIST) logos and identifiers to signify them as official agency publications
 - conform to the appropriate template as provided on the NVL website
 - be assigned publication numbers and DOIs
 - be permanently accessible and preserved in accordance with Public Access and records retention policies

RESPONSIBILITIES

Director, Information Services Office:

- Manages the publication of NIST Technical Series publications, including the *Journal of Research of NIST*.
- Creates and approves new series titles and descriptions.
- Closes and withdraws unused or outdated series titles.
- Establishes and carries out procedures for publishing and disseminating the NIST Technical Series Publications, including the *Journal of Research of NIST*.
- Manages the assignment of publication numbers and DOIs to individual publications within each series and individual articles in the *Journal of Research of NIST*.
- Ensures that the DoC seal and NIST logo and identifier are correctly used and placed on Technical Series Publications.
- Ensures that Technical Series Publications contain appropriate elements (e.g., cover, title page, publication number, author information) consistent with established publishing practices and standards.

- Manages the deposits of NIST scholarly and technical publications into the NIST public access repositories (PMC and FDSys) to ensure permanent access.
- Manages the transfer of digital copies of all Technical Series Publications to NARA according to the NIST Comprehensive Records Schedule to ensure permanent preservation.
- Manages the creation of bibliographic and descriptive metadata to facilitate discovery of individual Technical Series Publications and individual *Journal of Research of NIST* articles.

Authors

- Follow the instructions for preparing and submitting manuscripts for the [NIST Technical Series Publications](#) and the [Journal of Research of NIST](#) available on the NVL.
- Send Editorial Review Board-approved manuscripts slated for publication in any of the NIST Technical Series to the Information Services Office.
- Review and approve final version of document prior to publication by the Information Services Office.

DIRECTIVE OWNER

135 – Information Services Office, Management Resources

APPENDICES

A Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	2/24/16	Barbara Silcox	
Rev. .01	3/31/16	Dan Cipra	Formatting updates only
Rev. .02	5/24/2016	Barb Silcox	Updated with all DRB comments.

Records Management

NIST P 1600.00

Effective Date: 12/27/2016

PURPOSE

Establish the National Institute of Standards and Technology (NIST) program for managing records in compliance with the Federal Records Act (FRA), as amended, and other applicable authorities.

SCOPE

This directive addresses all records made or received by NIST.

LEGAL AUTHORITIES AND REFERENCES

- [Title 44 United States Code Chapter 31 \(Federal Records Act, as amended\)](#)
- [Title 36 Code of Federal Regulations Chapter XII Subchapter B](#)
- [OMB Managing Government Records Directive M-12-18](#)
- [Department of Commerce Administrative Order \(DAO\) 205-1, Records Management](#)


POLICY

The FRA, as amended, requires all federal agencies to make and preserve records containing adequate and proper documentation of their organization, functions, policies, decisions, procedures, and essential transactions. These records are Federal property, and it is the responsibility of every federal agency to manage them according to applicable laws and regulations.

NIST will meet this responsibility using centralized records management administered by the NIST Records Management Officer, under the NIST Chief of Staff, in coordination with all NIST Organizational Units (OUs) and NIST Associate Directors. This centralized records management program will be defined by planned, coordinated procedures, training, and activities needed for all staff to manage their recorded information.

As NIST migrates from a paper-based to an electronic records environment, the management of records continues to be an essential part of the mission. NIST will establish an approach to manage email records electronically. NIST will continue the transition to managing all permanent records in electronic format.

The NIST Associate Directors along with the NIST Chief of Staff shall ensure compliance by all OUs and staff with the NIST centralized records management program. The NIST Records Management Officer is delegated the authority to manage the NIST comprehensive records schedules and the overall centralized records management program.



Willie E. May
Director

12/27/16

Date

Web Content Policy

NIST P 1700.00
Effective Date: 11/29/2015

PURPOSE

The National Institute of Standards and Technology (NIST) websites are the “public face of NIST” and a critical communication vehicle for conveying accurate, clear, and concise information about NIST programs to external and internal stakeholders, and to provide data and research results.

This directive defines the overall NIST policy regarding publishing content on the external and internal NIST websites.

SCOPE

This directive applies to all NIST owned and maintained websites, including intranet sites not available to the public. This directive does not apply to NIST sites on Facebook, Twitter, and other social media, which are governed by the [Social Media directive \(N 1071.01\)](#). This directive also excludes collaboration sites created in the NIST enterprise-wide Microsoft 365 tool.

LEGAL AUTHORITIES AND REFERENCES

[Plain Writing Act of 2010](#), (Public Law 111-274, October 13, 2010)

[Government Performance and Results Modernization Act of 2010 \(H.R. 2142\)](#)

[Section 508 of the Rehabilitation Act of 1973](#), as amended (29 U.S.C. § 794 (d))

[The Copyright Act, 17 U.S.C. § 105](#)

[Paperwork Reduction Act of 1995 \(44 USC 3501-3520\)](#)

[Executive Order 13571—Streamlining Service Delivery and Improving Customer Service](#)

[President’s Memorandum on Transparency and Open Government](#) (January 2009)

[Memorandum M-10-23](#), Guidance for Agency Use of Third-Party Websites and Applications

President’s Memorandum [on Policies for Dot Gov Domain Issuance for Federal Agency Public Websites](#)

[Office of Management and Budget \(OMB\) Policies for Federal Agency Public Websites \(OMB M-05-04\)](#) and the related [OMB Circular A-130](#)

[OMB Memorandum M-11-24, Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service](#) (June 2011)

[OMB Privacy Guidance for Federal Websites](#)

[White House Digital Government Strategy](#)

[U.S. Digital Services Playbook](#)

[Department of Justice Guidance on the Privacy Act](#)

[DOC Public Communications Policy \(DAO 219-1\)](#)

[DOC Web Accessibility Requirements](#)

[DOC Endorsement Disclaimer Policy](#)

[DOC Offsite Notification Policy](#)

[DOC Policy Prohibiting Linking to Websites Related to Lobbying](#)

[DOC Policy on Privacy of Visitors to DOC Web Sites](#)

[DOC Privacy Policy Statements and Information Collection](#)

[DOC/OCIO Electronic and Information Technology Accessibility Policy](#)

[Department of Commerce Web Policies and Best Practices](#) (Mandatory and Recommended)

[DOC/OCIO Policy on the Approval and Use of Social Media and Web 2.0](#)

[DOC/OCIO Policy on the Paperwork Reduction Act and Information Collections Policy](#)

[Information Technology Security Program \(O 6102.00\)](#)

[NIST Web 2.0/Social Media Directive \(N 1071.01\)](#)

[NIST Public System Criteria \(S 6102.02\)](#)

[NIST Privacy Statement](#)

POLICY

All content posted on NIST internal and external websites must satisfy the Department of Commerce and NIST standards for data quality, IT accessibility, IT security and privacy, and effectively communicate to the intended audience.

The Public Affairs Office Director or designee is responsible for developing, implementing and maintaining requirements, processes, and procedures that ensure the content for internal and external websites is presented in accordance with all applicable standards.

 **NOV 29 2015**
Willie E. May _____ Date
Director

Web Content Requirements

NIST O 1701.00
Effective Date: 5/9/2016

PURPOSE

NIST's websites (both internal and external) are the public face of NIST and critical vehicles for conveying accurate, clear, and concise information to NIST stakeholders. This directive describes requirements needed to ensure that internal and external website content satisfies Department of Commerce (DOC) and NIST standards for data quality, IT accessibility, IT security and privacy, and effectively communicates to the intended audience(s).

APPLICABILITY

The following requirements are applicable for all NIST websites accessible to the public and all NIST staff, both external and internal, unless otherwise stated.

REFERENCES

[P 1700.00 NIST Web Content Policy](#)

DEFINITIONS

Accessibility – The ability of a website to deliver content to persons with disabilities (such as the visually or hearing impaired) in a manner that is “comparable to the access to and use of the information and data” by persons “who are not individuals with disabilities.” [Section 508 of the Rehabilitation Act \(29 U.S.C. 794d\), as amended by the Workforce Investment Act of 1998 \(P.L. 105-220\), August 7, 1998](#)

[Social Media/Web 2.0](#) – Online communities through which users share information, ideas, personal messages, and other content (such as videos and images).

[Information Coordinator](#) – A representative designated by, and accountable to, the director of each NIST Organizational Unit (OU) to serve on the NIST Information Coordinators Committee. The Information Coordinators Committee meets regularly (usually bimonthly) to review web-related issues and make recommendations on such issues to NIST management. The group is chaired by the Director of the Public Affairs Office (PAO) or their designee.

REQUIREMENTS

NIST OUs shall conform to all DOC/NIST mandatory policies, as previously stated in the NIST Web Content Policy [P 1700.00](#).

Accessibility. All NIST external and internal [websites](#) must be designed to ensure that persons with disabilities have access to, and use of, information and data in a manner that is comparable to the access and use available to persons without disabilities. Resources related to 508 compliance can be found on the [NIST internal forums](#).

Aliases and Redirects. All new requests for Office of Information Systems Management (OISM)-administered website aliases, third-level domains and redirects involving www.nist.gov addresses must be directed through the OU Information Coordinator to the Director of Public Affairs or their designee. Approvals will be granted jointly by PAO and OISM staff based on availability and appropriateness. On a yearly basis, OISM and PAO will provide each OU Information Coordinator with the current server configurations for their specific area for review and determination of configurations to be retired. Approvals for aliases, third-level domains and redirects will be considered on a case-by-case basis but will generally be accepted except when a dispute arises between organizations or the name might be easily misconstrued (e.g., irs.nist.gov or hate.nist.gov). Denials of approval may be appealed to the NIST Chief of Staff and the Associate Director for Management Resources. Appendix C provides details about what should be included in a request for an alias or redirect.

Analytics. In compliance with the [U.S. Digital Government Strategy](#), all NIST external sites are required to use analytics. The current code and information about implementing the analytics program on NIST websites are available from PAO.

Best Practices. It is the responsibility of all NIST website authors and managers to use accepted best practices for creating and managing websites. The U.S. Digital Service publishes [a list of best practices](#) for digital services and a [Content Guide](#) that should be consulted before creating new NIST websites.

Content Management Software (CMS). As a digital strategy for best practices and cost-effective management of NIST information, all content on external and NIST-wide internal websites shall be posted in the current enterprise-wide CMS.

This requirement applies to the majority of NIST web content, including, for example, descriptions of programs, research results, policies, procedures, publications, products, services, and training tutorials. The requirement to post NIST web content on the enterprise-wide CMS does not apply to collaboration sites created in the NIST enterprise-wide Microsoft 365 tool, datasets and web applications that: perform calculations or create simulations based on user input in real-time; must collect personally identifiable information (PII), payments or perform other sensitive transactions; or are restricted through passwords or other methods to designated small work groups.

If the current NIST CMS cannot support the functionality needed for a specific website or portion of a website, a business case for use of an alternative software must be approved by the Chief of Staff and the Chief Information Officer or their designee(s) prior to NIST use of the alternative software.

OUs with external or NIST-wide internal content not posted in the enterprise-wide CMS must receive approval for a content migration plan and timetable for migration to the NIST-wide CMS or receive a waiver from the Chief of Staff/Chief Information Officer within 90 days after the effective date of this order. Web content not posted in the NIST enterprise-wide system must adhere to all NIST/DOC requirements. The PAO will periodically review websites not in the central Content Management System to ensure that they are meeting NIST and DOC requirements. Any deficiencies found will be pointed out to the relevant OU and an agreed upon plan and timetable for remediation will be required.

Appendix B provides details as to what should be included in a CMS waiver request.

Copyrighted Material. Copyrighted material may be used on NIST webpages only after obtaining written permission from the owner, and the material must include the proper citations or attributions to the copyright holder.

Copyright protection is not available in the United States for most work prepared by an officer or employee of the United States Government as part of that person's official duties.

NIST authors must post peer-reviewed versions of manuscripts that have been accepted for publication in the central NIST publication database. However, NIST authors must not post the published version of the article on the NIST website without permission from the publisher. For articles published jointly with nongovernment authors, contributions from the nongovernment authors may be protected by copyright law. For more information, visit the [U.S. Copyright Office](#) website or contact the Office of the Chief Counsel for NIST (OCC).

Customer Satisfaction. [Executive Order 13571—Streamlining Service Delivery and Improving Customer Service](#) requires agencies to establish mechanisms to solicit customer feedback on government services and use such feedback to make improvements. The PAO Director or their designee is responsible for ensuring that NIST solicits web customers' feedback and distributes this feedback to NIST OUs to help ensure that NIST external websites respond to customer needs.

Data Disclaimers. A disclaimer has been approved by the Office of the Chief Counsel for NIST to cover delivery of data through NIST external websites. This disclaimer or a link to the disclaimer should be included on the entry pages for these data sets.

Data Disclaimer:

The National Institute of Standards and Technology (NIST) uses its best efforts to deliver a high-quality copy of the Database and to verify that the data contained therein have been selected on the basis of sound scientific judgment. However, NIST makes no warranties to that effect, and NIST shall not be liable for any damage that may result from errors or omissions in the Database.

OCC/NIST must approve any changes to this disclaimer prior to posting.

Domain Names. In accordance with Federal Management Regulation (FMR) [41 CFR Part 102-173](#) and in accordance with Office of Management and Budget (OMB) memorandum [M-05-04](#), all Department of Commerce domain names shall adhere to federal domain naming conventions, i.e., .gov, .mil, or .fed.us. Unless approved by the Secretary of Commerce, the use of .com, .org, .edu, .net, .biz, .tv, or other domains is prohibited.

New second-level domains not using 'NIST.GOV' format (e.g. [TOPIC].gov) may be requested using the [DOC Domain Request Form](#). Approvals will be granted jointly by PAO and OISM and then forwarded to DOC for approval. Denials of approvals at the NIST level may be appealed to the NIST Chief of Staff and the Associate Director for Management Resources. More information about DOC Domain Name policies can be found on the [DOC website](#).

New third-level domain names for external NIST websites should be directed, with a business case, through the OU Information Coordinator to the PAO Director or a designee. Appendix D provides information as to what information should be included in a request for a new third-level domain name.

Appendix A provides further clarification on the definitions of second-level and third-level domains.

Endorsements. All NIST external websites shall have a disclaimer stating that links to nonfederal government websites do not constitute endorsement of any product, service, organization, company, information provider, or content. Links to any commercial websites should be used only when information contained in those commercial websites is specifically related to NIST's research or services. NIST external websites should not include links to promotional information at a company. In some circumstances, it may be appropriate to provide credits, but not a link to a contract designer's promotional website. For further guidance, see DOC's [Endorsement Disclaimer Policy](#). NIST websites selected as award winners by commercial or other organizations may not display the awarding organization's logo on the NIST page. Factual information about the award may be provided.

Exit Scripts. All links directing a user to a nongovernment entity from a publicly accessible NIST website must include a disclaimer (exit script) informing that the user is leaving NIST/U.S. government web space. The exit script is automatically applied to all appropriate external links residing in the NIST central content management system (CMS). Code must be manually inserted for NIST sites/domains that are not in the CMS. [Information about how to obtain the exit script code](#) is available on NIST's intranet. Per the [DOC Offsite Notification Policy](#), exit scripts are not required on intranet sites.

Hosted Web Pages. NIST computers may be used to host web pages for outside organizations, provided: 1) these web pages facilitate the NIST mission; 2) NIST staff may participate in the outside organization as part of their official duties; and 3) the OU has authorized hosting such web pages. These web pages may include technical data, drafts of standards in preparation, reports, meeting minutes, committee announcements and other

information for public access and discussion. NIST does not have editorial control over the contents of such web pages, and normal review procedures of the information content by the Information Coordinators do not apply. However, these pages shall include a disclaimer similar to the following example:

"This information is made available through NIST information systems. However, the views expressed and the decisions reported do not necessarily connote NIST agreement with, or endorsement of them. Further, NIST does not endorse any commercial products that may be mentioned. Please address comments about this page to [insert group alias email]@nist.gov."

NIST may not host web pages that could result in financial gain to an outside organization or individual.

Also see Lobbying requirements below.

Lobbying. To comply with the [DOC Web Policy on Lobbying](#), NIST web pages may not link to web pages that engage in lobbying or encourage such activity. Also, NIST cannot host a website or web pages for any group or organization, if the hosted site or web pages engage in lobbying or link directly to any page that does, regardless of whether NIST has any control over the contents of the website.

NIST Identifier. The [NIST identifier](#) is comprised of the NIST logo followed by the words, U.S. Department of Commerce, National Institute of Standards and Technology (the "word mark.") External homepages of every NIST OU, division, program and office must feature a NIST web page identifier at the top of the page that links back to the NIST homepage at www.nist.gov. Please note: The NIST logo is a registered trademark and non-NIST organizations must have written approval to use it. Requests for use should be referred to the PAO Director or designee.

Plain Language. In accordance with the [Plain Writing Act of 2010](#) and the [President's Memorandum on Transparency and Open Government](#), NIST websites must communicate with clear and understandable language for the intended audience and be as accessible as possible for broad segments of the public. Use active verbs and concise, direct text. Proofread carefully. Before posting new web pages, check the readability of text with tools provided within Microsoft Outlook, Word, or other software tools. In addition, the federal government offers [tips, tools and training resources](#) on plain language.

Privacy. Consistent with the [DOC Policy on Privacy of Visitors to DOC Websites](#), all visitors to the NIST website must be assured that their privacy will not be violated as a consequence of viewing our web pages, information will not be taken from them or their computer without their knowledge, and their computer will not be compromised as a consequence of viewing our website. NIST websites must comply with the [Department of Justice Guidance on the Privacy Act](#) to ensure that existing privacy protections related to the collection, use and disclosure of personal information are followed. In addition, the Office of

Management and Budget (OMB) [requires website privacy statements](#) to include a disclosure about how they deal with any information that is collected.

To comply with these requirements and the [DOC's Privacy Policy Statements and Information Collection](#), all major points of entry and every publicly available page on NIST websites where any information is collected shall include a link to the [NIST Privacy and Accessibility Information Statement](#).

Surveys and Other Information Collection Activities. The Management and Organization Office (M&O) should be consulted to determine if the information to be collected is subject to the [Paperwork Reduction Act](#) (PRA). An OMB control number and approval statement may be required on surveys and information collection instruments.

Where web forms are used to collect information from web users, a link to the [NIST Privacy and Accessibility Information Statement](#) must be included such that the link is viewable without scrolling OR the link must be located adjacent to the "submit" button on the form. When multi-page forms are used, a link to the [NIST Privacy and Accessibility Information Statement](#) must be included such that the link is viewable without scrolling on the first page AND adjacent to any "submit" buttons.

If a website is directed toward children or information is knowingly collected from children, then the privacy statement must address the criteria stated in paragraph nine of the discussion section of [DOC Privacy Policy Statements and Information Collection](#).

Software and Applications (Apps) Disclaimer. A disclaimer must be posted on both NIST and non-NIST web pages that contain NIST-employee developed software or applications to provide acknowledgement of NIST work and state that the software is not subject to copyright in the U.S. A [software disclaimer](#) has been approved by the Chief Counsel for NIST to cover most applications.

OCC/NIST must approve any changes to this disclaimer prior to posting.

Sensitive Information. NIST web pages should continue to maintain a free and open exchange of scientific and technical information. At the same time, NIST web authors should carefully consider the sensitivity of content before it is posted and ensure that information related to topics such as national security and the privacy of individuals is appropriately protected. For help in determining the sensitivity of information, contact the relevant ITSO, OCC/NIST or the PAO Director, depending on the type of content sensitivity, for consultation and review.

Sensitive Programming Information. In support of privacy, web page source code should not contain information capable of identifying individual(s) responsible for the web page's development or maintenance, or their geolocation. When using software to develop a web page, any automatic settings pertaining to the identification or geolocation of the individual responsible for the web page's development or maintenance must be changed. An alias e-mail address can be provided for technical website questions. The source code should

include a contact for comments or inquiries regarding the content of the web page. In support of security, in so much as possible, a web page's source code should not provide supporting server and server configuration information.

RESPONSIBILITIES AND AUTHORITIES

NIST Chief of Staff (or designee)

- Review appeals of decisions regarding use of alternative software to the enterprise-wide content management system, for establishment of new domain names and aliases/redirects.

NIST Associate Director for Management Resources

- Review appeals of decisions regarding use of alternative software to the enterprise-wide content management system, for establishment of new domain names and aliases/redirects.

Director, Public Affairs Office (or designee)

- Serves on the Department of Commerce Web Advisory Council Group. Chairs Information Coordinators group and coordinates information flow of web-related policies and procedures to OU level. Manages content of NIST-level external and internal websites. Communicates directive policy and procedures to NIST stakeholders, works to ensure accuracy of content, collects feedback from website customers, works to implement improvements responsive to that feedback, and serves as the administrative point of contact in gathering of requirements and review by stakeholders for content-related web initiatives.
- Approves requests jointly with the Chief Information Officer for enterprise-wide content management waivers, new aliases and redirects, and domain names.

Chief Information Officer (or designee)

- Serves on the Department of Commerce Web Advisory Council Group. Manages all information technology related aspects of NIST's external and internal websites, including security and privacy policies and procedures.
- Approves requests jointly with the Public Affairs Director for enterprise-wide content management waivers, new aliases and redirects, and domain names.

Management and Organization Office

- Assists with Privacy Act and Paperwork Reduction Act compliance.

Office of the Chief Counsel

- Assists with legal compliance as described above, including copyright reviews, and approvals of data and software disclaimers.

Information Coordinators

- Oversee processes to ensure the accuracy of website content and compliance with NIST and DOC website policies for individual NIST OUs. Provide information and guidance on policy and best practices to individual OU-based web content page authors. Review content for privacy. Individual OUs may assign additional responsibilities as appropriate.

DIRECTIVE OWNER

100 – Chief of Staff, with delegation to 107, the Public Affairs Office (PAO), and 180, the Office of Information Systems Management (OISM)

APPENDICES

- A. Domain Name Definitions
- B. CMS Waiver Request Form
- C. Alias/Redirect Request Form
- D. Domain Name Request Form
- E. Revision History

APPENDIX A

Domain Name Definitions

Top-Level Domain Names – .gov, .mil, or .fed.us are all top-level domains.

Second-Level Domain Names – second-level domain names appear immediately to the left of the dot and domain name extension.

In nist.gov, nist is the second-level domain of the .gov top-level domain

Third-Level Domain Names – third-level domains appear immediately to the left of a second-level domain.

In nccoe.nist.gov, nccoe is the third-level domain name.

APPENDIX B

CMS Waiver Requests

Requests for a waiver out of the NIST-wide CMS must include the following information and must be submitted by your Information Coordinator.

OU:

OU Information Coordinator:

Signature of OU Director:

Requestor Name:

Requestor Phone Number:

Requestor Email Address:

Address of website needing waiver:

Target audience of website:

Purpose of website:

Do you plan to use a different CMS? If so, what CMS?

Business case: Please provide a business case for why you need a waiver. Your business case should include information about the unique functionality required for your site/content that you believe cannot be fulfilled by the central NIST CMS.

APPENDIX C

Alias/Redirect Requests

Requests for aliases/redirects must include the following information and must be submitted by your Information Coordinator.

OU:

OU Information Coordinator:

Requestor Name:

Requestor Phone Number:

Requestor Email Address:

Current address of website needing redirect:

Address you would like to redirect to:

Business case: Please provide a business case for why you need a redirect. Your business case should include:

- Number of page views and unique visitors to your site during the past six months.
This information can be found using Google Analytics. If you are not familiar with Google Analytics, please work with your Information Coordinator to obtain this information.
- What purpose will the redirect serve?

APPENDIX D

Domain Name Requests

Requests for new third-level domain names must include the following information and must be submitted by your Information Coordinator.

OU:

OU Information Coordinator:

Signature of OU Director:

Requestor Name:

Requestor Phone Number:

Requestor Email Address:

Requested new domain name:

If the site already exists at another address, current address:

Business Case: Please provide a business case for why your site requires a third-level domain name. That business case should include:

- Purpose of domain/site
- Primary audience
- Reasons why a third-level domain is needed

APPENDIX E

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	3/14/2014	Jenny Covahey	
Ver .01	8/15/2014	Dan Cipra	Formatting updates
Ver. 02	8/29/2014	Gail Porter	Response to OISM comments
Ver. 03	9/30/2014	Gail Porter	Response to Information Coordinator discussion
Ver. 04	11/20/14	Gail Porter	Response to Information Coordinator written comments
Ver. 05	12/23/14	Gail Porter	Added 4 references with links, added one missing link
Ver. 06	7/1/2015	Gail Porter	Response to NIST OCC and DOC OGC review. Made more than 30 changes mostly related to legal authorities, requirements, formatting, and clarity of requirements.
Ver. 07	2/23/2016	Robin Materese	Reviewed and updated document after passage of Web Policy. Changes mostly related to adding links, and copyedits. Added appendices as to what information should be included in various requests.
Ver. 08	3/24/2016	Robin Materese	Updates based on feedback from Directives Review Board.
Ver. 09	4/07/2016	Robin Materese	Additional updates made based on feedback from Directives Review Board.

Review of Fundamental Research Communications

NIST P 1800.00

Effective Date: 7/5/2016

I. PURPOSE

This directive establishes a governing policy for review and approval prior to the occurrence of a fundamental research communication.

II. SCOPE

The requirements set forth in this policy apply to fundamental research communications.

A “fundamental research communication” is “a public communication [defined below] that relates to the Department’s programs, policies, or operations and takes place or is prepared officially and that deals with the products of basic or applied research in science or engineering, the results of which ordinarily are published and shared broadly within the scientific community, so long as the communication does not contain information that is proprietary, classified, or restricted by federal statute. If a communication also includes matters of policy, budget, or management, then it is not a Fundamental Research Communication.” [\[DAO 219-1\]](#).

A “public communication” is “any communication that is intended for, or should reasonably be expected to have, broad distribution outside the U.S. Government, including without limitation: public speeches, news releases and advisories, news conferences, broadcast appearances, and interviews or discussions with journalists; public writings, such as articles or papers in publications or other writings distributed through mass-mailing, e-mail, or posting on a website; public educational instruction and/or lectures, conferences, seminars, etc.; and public distribution of audiovisual works, including without limitation slide sets, PowerPoint presentations, multimedia (i.e., any combination of two or more media productions), and exhibits.” [\[DAO 219-1\]](#)

These requirements apply to communications that

- take the form of scholarly and technical publications of text, software, data, and videos in all media including but not limited to the NIST Technical Publications series, hardcopy print media, and machine-readable media; and
- contain new findings from NIST technical programs that have not been previously reviewed.

This policy applies to all NIST staff, including full- and part-time employees, temporary government employees, and special government employees.

This policy does not apply to communications that are not intended for, or would not be reasonably expected to have, broad distribution outside the U.S. Government. Such non-public communications include the exchange of information with individuals, including collaborators, and similar interactions within our scientific and technical communities.

This policy does not apply to non-official communications of interest, which are defined in and managed in accordance with [DAO 219-1](#).

This policy does not apply to public information provided to the news media and general audiences, including the NIST website, managed in accordance with NIST [O 1074.00](#)
Public Communications

This policy does not apply to review of NIST webpages, which are managed in accordance with [NIST O 1701.00](#) Web Content Requirements. However, fundamental research communication must be reviewed before it is provided on a publicly accessible webpage (NIST or non-NIST).

III. LEGAL AUTHORITY

- A. [15 U.S.C. § 272\(c\)\(17\), National Institute of Standards and Technology Act – Implementation Activities](#)
- B. [15 U.S.C. §§ 290-290f, Standard Reference Data Act](#)
- C. [44 U.S.C. § 3501 et seq., Paperwork Reduction Act of 1995](#)
- D. [Public Law 110-69 America COMPETES Act](#)
- E. [Department Administrative Order \(DAO\) 201-21, Commerce Metric Conversions](#)
- F. [Department Administrative Order \(DAO\) 202-751, Discipline](#)
- G. [Department Administrative Order \(DAO\) 219-1, Public Communications](#)
- H. [NIST O 5101.00 NIST Scientific Integrity](#) (1/17/2013)
- I. [National Institute of Standards and Technology Guidelines, Information Quality Standards, and Administrative Mechanism](#)

IV. POLICY

NIST requires that an effective quality management system is in place and functioning during the process that ends with a fundamental research communication. To this end, NIST policy requires:

- A. Authorization within the originating Organizational Unit (OU) prior to release of all fundamental research communications;
- B. Authorization by the Editorial Review Board prior (ERB) to release of fundamental research communications that take the form of scholarly or technical publications (see NIST O 1801.00);

- C. Reporting of all NIST measurement results with accompanying quantitative statements of uncertainty;
- D. Reporting of all NIST measurement results using the International System of Units (SI); and
- E. Inclusion of an appropriate disclaimer when identification of a commercial product or entity in a communication is necessary.
- F. Inclusion of a statement that the research was reviewed and approved by the human subjects and/or vertebrate animal review process before research involving human or animal subjects was conducted. (See [NIST P 5500](#) Human Subjects Protections and [NIST O 5501](#) Human Subjects Protection Program and NIST policy for Humane Care and Treatment of Vertebrate Animals.)

The NIST Director delegates authorization for release of fundamental research communications to the Chair of ERB when publication is intended. OU Directors may require that they give final approval following ERB approval. If this option is exercised, and additional changes in a fundamental research communication are needed, ERB must be advised. For documents that do not require ERB approval prior to release (see NIST O 1801.00), final authorization for release is delegated by the NIST Director to the OU Directors, who may also delegate this authority. Editorial Review Board decisions may be appealed through the author's management chain to the appropriate Associate Director.

Authors found in violation of this policy may be disciplined by their management in accordance with [DAO 202-751](#).

 _____ Willie E. May Director	07/05/16 _____ Date
--	---------------------------

Review of Fundamental Research Communications

NIST O 1801.00
Effective Date: 7/5/2016

PURPOSE

This Order describes the requirements and responsibilities for review and approval prior to the release of a fundamental research communication.

APPLICABILITY

This Order applies to fundamental research communications as defined in NIST P 1800.00.

REFERENCES

[Department Administrative Order \(DAO\) 219-1, Public Communications](#)

[NIST P 1800.00 NIST Review of Fundamental Research Communications](#)

[NIST O 1005.00 Administrative Committees](#)

[NIST O 1074.00 Public Communications](#)

[NIST Special Publication 330, The International System of Units](#)

[NIST Special Publication 811, The NIST Guide for the Use of the International System of Units](#)

[NIST Technical Note 1297, Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results](#)

[Editorial Review Board \(ERB\) Charter](#)

DEFINITIONS and ACRONYMS

Editorial Review Board (ERB) – ERB is a NIST Standing Administrative Committee as defined in [O 1005.00 Administrative Committees](#) and described in the [Editorial Review Board Charter](#).

Editorial Review System (ERS) – The ERS is the information management system through which fundamental research communications intended for publication are reviewed and approved. This system has a mechanism for uploading revisions and reviewers' comments as well as tracking a communication's approval history.

Fundamental Research Communication – A fundamental research communication is a public communication that relates to the Department's programs, policies, or operations and takes

place or is prepared officially and that deals with the products of basic or applied research in science or engineering, the results of which ordinarily are published and shared broadly within the scientific community, so long as the communication does not contain information that is proprietary, classified, or restricted by federal statute. If a communication also includes matters of policy, budget, or management, then it is not a fundamental research communication.¹

Official Communication – Official communications are those that are prepared by a NIST staff member or Associate engaged in research activities at or for NIST (to the extent allowed by law and the terms of the Associate's agreement) under any of the following conditions:

At the direction of a superior;

During official working hours;

With use of U.S. Government resources; or

With assistance of U.S. Government employee(s) on official duty.¹

Public Communication – Any communication that is intended for, or should reasonably be expected to have, broad distribution outside the U.S. Government, including without limitation:

Public speeches, news releases and advisories, news conferences, broadcast appearances, and interviews or discussions with journalists;

Public writings, such as articles or papers in publications or other writings distributed through mass-mailing, e-mail, or posting on a website;

Public educational instruction and/or lectures, conferences, seminars, etc.; and

Public distribution of audiovisual works, including without limitation slide sets, PowerPoint presentations, multimedia (i.e., any combination of two or more media productions), and exhibits.¹

Quality Management Objectives – Scientific and technical information disseminated by NIST is presented in a clear, complete, and unbiased manner. Conclusions are supported by data and observations. Figures and tables are correct, clear, useful, necessary, and properly labeled. Manuscripts are organized efficiently and appropriately and contain proper syntax, grammar, and spelling. Acronyms are used sparingly and defined properly the first time that they are used. Results are reliable and accurate to an acceptable degree of error.²

¹ [Department Administrative Order \(DAO\) 219-1, Public Communications](#)

² See also [National Institute of Standards and Technology Guidelines, Information Quality Standards, and Administrative Mechanism](#)

REQUIREMENTS

As an agency of the Federal Government and in the interest of maintaining NIST's reputation for producing high-quality work products, fundamental research communications must be reviewed, as delineated below, prior to the communication occurring:

- A. Fundamental research communications must be reviewed to ensure their technical and editorial quality.
- B. Fundamental research communications that require Organizational Unit (OU) and ERB review and approval prior to release include the following:
 - 1. Journal manuscripts, including manuscripts intended for publication in traditional print journals, on the Internet, and in on-line or open access journals;
 - 2. Book chapters;
 - 3. Books;
 - 4. Conference and workshop proceedings;
 - 5. Extended abstracts (as defined by meeting organizers but typically two to six pages in length and published in a citable location);
 - 6. NIST Technical Series publications (e.g., Special Publications, Internal/Interagency Reports, Journal of Research of NIST);
 - 7. Documents, including "pre-prints," slides, and presentations, that will be posted to NIST and non-NIST websites that are publicly accessible. However, slides and presentations (1) posted to a restricted-access website or (2) made available only to meeting attendees or (3) derived from fundamental research communications that were approved by ERB do not require ERB review and approval but do require OU approval; see Sections IV G 5 and IV G 6.
 - 8. Encyclopedias;
 - 9. Technical documents that are posted as final drafts for public review;
 - 10. Users' manuals for software;
 - 11. Dataset documentation;
 - 12. Videos describing results of NIST's technical programs; and
 - 13. Other scholarly and technical publications of similar stature.
- C. Individualized review requirements for the above types of fundamental research communications are provided in the draft linked suborders:
 - 1. NIST S 1801.01 Review of Scholarly and Technical Manuscripts Intended for Publication;
 - 2. NIST S 1801.02 Review of Data Intended for Publication;

3. NIST S 1801.03 Review of Software Intended for Publication; and
 4. NIST S 1801.04 Review of Scholarly and Technical Videos Intended for Publication.
- D. Fundamental research communications that are intended to be made public but do not require a full OU and ERB review are categorized as “Notings” because the OU and ERB acknowledge their existence. Notings include the following:
1. Manuscripts for publication in the Journal of Physical and Chemical Reference Data (JPCRD) that do not include NIST authors and that have been reviewed and found to meet journal requirements in the JPCRD peer-review process. (JPCRD manuscripts from NIST authors follow the normal editorial review process.)
 2. Federal Information Processing Standards that have been through the standards development cycle, reviewed, and received Secretarial approval;
 3. Bibliographies and appendices that are published routinely to update an established series of such publications;
 4. Articles and other fundamental research communications, excluding presentations, that are extracted from previously approved communications (See Section IV G 6);
 5. Errata;
 6. Changes to information in previously reviewed and approved documents;
 7. Publications in a language other than English that are not accompanied by an English translation; and
 8. Other publications of similar stature.
- E. Notings are acknowledged by the Division Chief (or Office Director or Center Director in OUs without a division structure), the ERB sponsor, and the ERB Chair. Fundamental research communications that are being noted must be approved for release by the ERB Chair before the communication occurs.
- F. Division Chiefs (or Office Directors or Center Directors in OUs without a division structure) certify [Homeland Defense Clearance](#) for all fundamental research communications.
- G. Fundamental research communications that require review and approval within the appropriate OU (which may occur at a lower organizational level if so delegated by the OU Director) but do not require ERB approval prior to release include the following:
1. Brochures and pamphlets;
 2. Newsletters and contributions to newsletters;

3. Technical documents that are posted iteratively (as a series of drafts) for public input;
 4. Abstracts (as defined by meeting organizers, but typically no more than 1 page in length);
 5. Speeches, presentations, and posters that are not intended to be published or posted to a publicly accessible website, but which may be posted to a website to which access is limited (e.g., accessible only to meeting attendees);
 6. Speeches, presentations, and posters that are derived from fundamental research communications that were previously reviewed and approved by ERB.
 7. Grant/Contractor Reports (the only NIST Technical Series publication type that does not go through ERB because NIST staff were not involved in its preparation or content);
 8. Non-NIST papers acknowledging NIST involvement (e.g., NIST membership on a committee that has authored the paper) if NIST is given an opportunity to review a draft;
 9. Voluntary consensus standards if NIST is given an opportunity to review a draft;
 10. Program criteria;
 11. Letters to the Editor;
 12. Editorials;
 13. Obituaries;
 14. Letters, faxes, e-mails, etc. containing previously unreviewed fundamental research communications;
 15. Software (but users' manuals must be reviewed as technical publications);
 16. Datasets, including Standard Reference Data (but documentation for users is reviewed as a technical publication);
 17. Calibration reports;
 18. Reports of Analysis;
 19. Certificates of Analysis and other certificates that accompany Standard Reference Materials (SRMs), Reference Materials (RMs), and Standard Reference Instruments (SRIs); and
 20. Other communications of similar stature.
- H. For fundamental research communications that do not require ERB review, individualized review processes are established by the OUs. Review and approval may be delegated to lower organizational levels. The OU is responsible for

ensuring that all ERB policy and editorial requirements (e.g., disclaimers, SI units, human subjects research approvals) are met. Preliminary results that are shared should include a statement that the results, including the uncertainty analysis, are subject to revision.

- I. The Public Affairs Office should be advised by the OU of publications that may relate to a public controversy, or which could be reasonably foreseen to create one.
- J. Fundamental research communications that involve human subjects and/or vertebrate animals must have documented applicable human subjects or animal research review and approval, as required under NIST O 5501 Human Subjects Protection Program and the NIST policy for Humane Care and Treatment of Vertebrate Animals.
- K. Reviewers must use the Editorial Review System to review and approve fundamental research communications that are intended for publication. If changes are numerous or might prevent a paper from being approved, the reviewer should ask the author to make changes and upload a revised version to the Editorial Review System so that subsequent reviewers can review a more final form of the communication.
- L. Approval or non-approval shall not be based on the policy, budget, or management implications of the communication.
- M. Fundamental research communications that have been submitted to a publisher without prior approval for release are categorized as “communicated without approval” and the author’s Division Chief or Center or Office Director is notified by the ERB Chair that this has occurred. (The Division Chief or Center or Office Director is responsible for taking any appropriate follow-up action.)
- N. All NIST measurement results must comply with directives related to the evaluation and expression of measurement uncertainty (see NIST Technical Note 1297).
- O. All NIST measurement results must be reported using the International System of Units (SI) and SI style as described in NIST Special Publication 811. When the field of application or the special needs of users require the use of non-SI units, the values of quantities are first stated in SI units and the corresponding values expressed in non-SI units follow in parentheses.
- P. NIST does not evaluate commercial products unless such an evaluation is part of a formal agreement. Such formal agreements are established in consultation with the Office of the Chief Counsel for NIST. If it is necessary to report information concerning commercial products, methods, processes, or organizations in connection with the performance of a mandated responsibility of NIST or a contract from another agency, identification of the commercial products, processes, or organizations should be coded to control the distribution of that information.

- Q. The use of trade and product names should be avoided in all fundamental research communications (including illustrations) except where mention of the name is essential to the comprehension or replication of the reported results or where public safety or health is involved. Generic terminology should be used wherever possible in lieu of specific commercial identification. A disclaimer must be included if a commercial product is mentioned.

Example: Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

- R. When a fundamental research communication presents information that could be mistakenly construed to represent an official position of NIST or the United States Government, a disclaimer must be included.

Example: These opinions, recommendations, findings, and conclusions do not necessarily reflect the views or policies of NIST or the United States Government.

- S. When a NIST author uses copyrighted material in a fundamental research communication, the author must obtain permission for use from the copyright holder and indicate that the material is copyrighted. A reference can be provided to the original source material.

Example: Copyright [insert name of copyright holder]; used with permission.

- T. If a NIST author intends to publish in a foreign journal, the foreign journal must be accessible in the United States and must originate in a country that is [diplomatically recognized by the United States](#). Manuscripts in languages other than English must be translated into English for review and approval by ERB; otherwise they will be noted.

RESPONSIBILITIES

NIST Director:

1. Is responsible for review prior to release of a fundamental research communication.
2. Delegates this responsibility to the Chair of ERB if the fundamental research communication is intended for publication.
3. Delegates this responsibility to the OU Director if the fundamental research communication is of a type that does not go through ERB.
4. Appoints the ERB Chair.

NIST Associate Directors:

1. Ensure compliance with the fundamental research communications directives.

2. Approve release of fundamental research communications that may relate to a public controversy, or which could be reasonably foreseen to create one.

Organizational Unit (OU) Directors:

1. Ensure compliance with the fundamental research communications directives by staff performing technical activities under their direction.
2. Establish OU requirements and procedures for assuring the technical and editorial quality of fundamental research communications prepared by staff members who report to them.
3. Establish OU policies and procedures to authorize release of fundamental research communications prepared under their supervision based on a determination that the communications meet the quality management objectives of this Order.
4. May delegate authority to authorize release of fundamental research communications
5. Establish and communicate requirements for reviews and approvals for release that are delegated.
6. Provide specific approval of books and book chapters, reports of information pertaining to commercial products, reports of new values of basic physical standards or fundamental constants, and publications that may relate to a public controversy, or which could be reasonably foreseen to create one.
7. Ensure that the Chief of the Public Affairs Office is advised of upcoming publications that may relate to a public controversy, or which could be reasonably foreseen to create one.
8. Nominate ERB members.

Division Chiefs, Office Directors, and Center Directors:

1. Ensure compliance with the fundamental research communications directives by staff performing technical activities under their direction.
2. Assure the technical and editorial quality of fundamental research communications prepared by staff members who report to them.
3. Ensure that appropriate ethical and regulatory review approvals for activities involving human subjects and/or live vertebrate animals has been obtained.
4. Certify [Homeland Defense Clearance](#) for technical publications.
5. Authorize release of fundamental research communications prepared under their supervision based on a determination that the communication meets the quality management objectives of this Order.
6. If so delegated by the OU Director, may provide final review and approve the release of fundamental research communications that are prepared under their

supervision and that do not require ERB review. This approval must be based on a determination that the communication meets the quality management objectives of this Order.

7. May delegate authority to approve release of fundamental research communications that do not require ERB review.
8. Identify issues to OU management or the ERB Chair that may adversely affect the reputation of NIST and require additional levels of review.

Other Supervisors (e.g., Group Leaders, Program Managers):

1. Ensure compliance with the fundamental research communications directives by staff performing technical activities under their direction.
2. Assure the technical and editorial quality of fundamental research communications prepared by staff members who report to them.
3. Ensure that appropriate ethical and regulatory review approvals for activities involving human subjects and/or live vertebrate animals has been obtained.
4. If so delegated, may provide final review and approve the release of fundamental research communications that are prepared under their supervision that do not require ERB review. This approval must be based on a determination that the communication meets the quality management objectives of this Order.
5. Identify issues to OU management or the ERB Chair that may adversely affect the reputation of NIST and require additional levels of review.

Authors:

1. Prepare fundamental research communications that are high quality, technically accurate, and editorially correct.
2. Are responsible for the correctness of the technical results being reported.
3. Are responsible for obtaining prior appropriate ethical and regulatory review approvals for activities involving human subjects and/or live vertebrate animals
4. Report the results of their technical work using the International System of Units (SI) and its proper usage as described in NIST SP 811.
5. Include quantitative statements of uncertainty with their measurement results.
6. Identify issues to OU management or the ERB Chair that may adversely affect the reputation of NIST and require additional levels of review.

Reviewers of Fundamental Research Communications:

1. Review and approve fundamental research communications intended for publication, primarily checking for technical quality.

Editorial Review Board:

1. Reviews and approves fundamental research communications intended for publication, primarily checking for editorial quality and compliance with NIST policy.

Office of the Chief Counsel for NIST:

1. Interprets laws and regulations that affect NIST publication activity.
2. Reviews and approves fundamental research communications that provide evaluations of commercial products, checking for legal issues and compliance with NIST policy.
3. Reviews and approves fundamental research communications reporting on results of disaster investigations, checking for legal issues and compliance with NIST policy.
4. Reviews and approves any other fundamental research communications as requested by OU Directors or ERB.
5. Provides disclaimers when examples in Section IV are inadequate.

Engineering Laboratory Director:

1. Reviews and approves fundamental research communications reporting on results of disaster investigations, even when those investigations are conducted in OUs other than the Engineering Laboratory

Human Subjects Protection Office:

1. Verifies that work involving human subjects and/or vertebrate animals that is described in a fundamental research communication has received appropriate ethical review and approval.

Public Affairs Office

1. Answers public inquiries related to fundamental research communications

DIRECTIVE OWNER

602 – Editorial Review Board Chair

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	1/30/14	Katherine Sharpless	Initial draft
Rev. .01	2/2/16	Dan Cipra	Formatting updates only
Rev. .02	4/7/2016	Katherine Sharpless	Incorporated DRB and ADLP changes

Review of Scholarly and Technical Manuscripts Intended for Publication

NIST S 1801.01
Effective Date: 07/26/2016

PURPOSE

This directive describes the requirements for review of fundamental research communications in the form of manuscripts that are intended for publication in any media including on pre-print servers and in electronic journals.

APPLICABILITY

This suborder applies to all NIST staff, including full- and part-time employees, temporary government employees, and special government employees.

REFERENCES

- [NIST O 1801.00 NIST Review of Fundamental Research Communications](#)
- [NIST O 1005.00 Administrative Committees](#)
- [Editorial Review Board Charter](#)

DEFINITIONS

In the context of this directive, the term “manuscript” includes any of the following:

- A paper intended for publication in a traditional print journal, on the Internet, or in an on-line or open access journal
- A book chapter
- A book
- Conference or workshop proceedings
- An extended abstract
- A NIST Technical Series publication
- A document such as a “pre-print,” slides, or a presentation that will be posted to a publicly accessible website
- An encyclopedia or encyclopedia entry

- A technical document that is posted as a final draft for public review
- A user's manual for software
- Dataset documentation
- Any other scholarly and technical publications of similar stature.

REQUIREMENTS

1. The originating OU has primary responsibility for the editorial quality of the manuscript as well as the quality of the technical information to be published. (The originating OU for a manuscript is the OU of the corresponding or senior NIST author unless there is agreement to a different arrangement.) Review and approval within the originating OU are required to ensure that a manuscript is complete and that revisions necessary to meet NIST quality requirements have been made. Review within the originating OU must thoroughly address technical content, editorial quality, and policy issues.
2. Manuscripts presented to the Editorial Review Board (ERB) must be approved in the Editorial Review System. In every case, the approval of the Division Chief (or equivalent) must be recorded, indicating that the manuscript has been reviewed and approved in the originating OU.¹
3. Errors in typing, spelling, grammar, organization, format, technical expression, and policy should be identified and corrected before the manuscript is submitted to the Editorial Review Board. If excessive errors of this kind are present, the manuscript may be returned to the author for corrections before it is accepted by ERB for review.
4. ERB review consists of review and approval by
 - one or more ERB readers, one of whom must be external to the originating division unless permission to use a division member is approved by the ERB Sponsor, the ERB Chair, or the OU Director,
 - the designated ERB Sponsor, and
 - the ERB Chair.
5. In special cases as described in NIST O 1801.00, additional reviews may be required.

For a noting, review and approval by the Division Chief (or equivalent), ERB Sponsor, and ERB Chair are required. Review and approval by an ERB reader is not necessary.

The ERB reader(s) of a manuscript must not be involved in the technical work, the documentation, or their direct supervision. The ERB reader(s) may not be from the same division as the paper's primary author(s) unless permission is granted by the ERB Sponsor, ERB Chair, or OU Director.

¹ Note that completion and retention of a NIST-114 is no longer required.

ROLES AND RESPONSIBILITIES

Authors

- Prepare manuscripts that are of high quality, technically accurate, and editorially correct.
- Report the results of their technical work using the International System of Units (SI) and appropriate statements of uncertainty.
- Are responsible for the correctness of technical results.
- Are responsible for determining whether or not a manuscript raises substantive and sensitive policy issues even for projects that have not themselves been designated as sensitive. If there are sensitive or policy issues, staff members shall provide their Division management and OU Management with oral or written reports and include NIST Counsel if appropriate after consulting with OU Management, before making any disclosure of findings or conclusions to sponsors or others outside of NIST.
- Suggest Editorial Review Board readers when submitting a manuscript to ERB via the Editorial Review System (in consultation with co-authors, division chiefs, and others as appropriate). Persons suggested should be technically informed about the subject, objective, and removed from any conflict of interest that might arise from working in the organizational environment(s) of the author(s).

OU Management (Directors, Division Chiefs, Group Leaders)

- Reviews and approves manuscripts, checking for technical quality as well as editorial and policy issues.
- Examines manuscripts for consistency with NIST statutory authority and operating policies; appropriateness of selected medium for publication; appropriate recognition of sponsors, institutions, and persons; and other relevant matters.

Editorial Review Board Readers

- Review and approve manuscripts, checking for technical quality as well as editorial and policy issues.
- Provide critical evaluation of the technical content and methodology, statistical treatment of data, uncertainty analysis, use of appropriate reference data and units, and bibliographic references.
- Examine manuscripts for writing quality and correct use of language, freedom from jargon, clarity of expression, effective organization, good format, appropriate title, adequate references, indexing, citations, footnotes, and figures.
- Are encouraged to communicate directly with authors regarding their comments and suggestions. However, in unusual cases, readers may choose to remain anonymous. In this case, unsigned comments are sent to the paper's ERB Sponsor.

Editorial Review Board Sponsors

- Confirm suitability of Editorial Review Board Reader as selected by the author or the author's superior(s).
- Review and approve manuscripts, checking for editorial and policy issues as well as technical quality, as applicable. Sponsors' recommendations may include the need for additional technical or management review including recommendations that management request legal review.
- Examine manuscripts for writing quality and correct use of language, freedom from jargon, clarity of expression, effective organization, good format, appropriate title, adequate references, indexing, citations, footnotes, and figures.
- Examine manuscripts for consistency with NIST statutory authority and operating policies; appropriateness of selected medium for publication; appropriate recognition of sponsors, institutions, and persons; and other relevant matters.
- When necessary, arbitrate differences of opinion between readers and authors, recommend additional readers if required, or take other steps to resolve issues.

Editorial Review Board Chair

- Approves the release of manuscripts intended for publication.
- When necessary, arbitrates differences of opinion between readers and authors, recommends additional readers if required, or takes other steps to resolve issues.

DIRECTIVE OWNER

Division 602 – Editorial Review Board Chair

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	04/01/14	Katherine Sharpless	Initial draft
Rev. .01	8/3/2016	Dan Cipra	Formatting updates only

Review of Data Intended for Publication

NIST S 1801.02
Effective Date: 12/6/2016

PURPOSE

This suborder provides requirements for review of data that will be made publicly available.

APPLICABILITY

This suborder applies to all NIST staff, including full- and part-time employees, temporary government employees, and special government employees.

REFERENCES

- [NIST O 1801.00 NIST Review of Fundamental Research Communications](#)
- [NIST O 1005.00 Administrative Committees](#)

DEFINITIONS

Data - Research data means the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or communications with colleagues. This “recorded” material excludes physical objects (e.g., laboratory samples). Research data also does not include:

- Trade secrets, commercial information, materials necessary to be held confidential by a researcher until they are published, or similar information which is protected under law; and
- Personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study.¹

For purposes of this suborder, NIST considers the contents of laboratory notebooks to be preliminary analyses.

Enterprise Data Inventory (EDI): The Enterprise Data Inventory is the database in which metadata describing NIST data assets resides and in which users designated by organizational unit (OU) management approve a dataset for publication.

¹ [2 C.F.R. §200.315 \(e\)\(3\)](#)

REQUIREMENTS

1. The OU in which data is prepared for public release is responsible for establishing processes and procedures for ensuring the technical quality of the work and the associated review and approval prior to publication, including, as appropriate:
 - correctness of the data reported to the user;
 - accuracy of the data;
 - completeness of the provenance;
 - completeness and effectiveness of documentation that makes it possible for users to use the data.
2. If a free-standing dataset is being published, OU approval is required. If the dataset is associated with a publication (e.g., published as supplemental information), the dataset accompanies the manuscript when it is reviewed under NIST S 1801.01. If the dataset is being published with associated documentation (e.g., a user manual), the OU is responsible for the quality of the data itself and the NIST Editorial Review Board is responsible for editorial review of the associated documentation under NIST S 1801.01.
3. Datasets and associated documentation must comply with NIST policies for technical publications, including descriptions of measurement uncertainties and disclaimers where appropriate, as well as the use of SI units. Documentation that supports the use of NIST data that is made available to the public must include, as appropriate:
 - a description of the data;
 - a description of data tables;
 - a statement describing how to obtain the data;
 - operating system requirements for executable programs;
 - specification of applications programs required to access and use any of the files associated with the data;
 - statement of inputs required from the user;
 - statement concerning technical support available from NIST with appropriate contact information; and
 - the disclaimer found at <http://www.nist.gov/open/license.cfm> or another suitable disclaimer as approved by the Office of Chief Counsel for NIST

ROLES AND RESPONSIBILITIES

Authors

- Prepare datasets and associated documentation that are of high quality, technically accurate, and editorially correct.
- Report the results of their technical work using the International System of Units (SI) and appropriate statements of uncertainty.

- Are responsible for the correctness of technical results.
- Provide reviewers with access to the data via an appropriate medium (e.g., CD, link), coded ('readme') text files if they exist, and the documentation manuscript.
- Are responsible for determining whether or not a technical publication of datasets and associated documentation raises substantive and sensitive policy issues even for projects that have not themselves been designated as sensitive. If there are sensitive or policy issues, staff members shall allow responsible management to review oral or written reports and include NIST Counsel, if appropriate, before making any disclosure of findings or conclusions to sponsors or others outside of NIST.

Division Chiefs, Office Directors, and Center Directors:

- Are responsible for authorizing release of fundamental research communications in the form of data prepared by staff members who report to them.
- May delegate authority to approve release of fundamental research communications in the form of data prepared by staff members who report to them.

Other Supervisors (e.g., Group Leaders, Program Managers):

- If so delegated, may provide final review and approve the release of fundamental research communications in the form of data that are prepared under their supervision.

Editorial Review Board Readers, Sponsors, and Chair:

- Are responsible for review and approval of manuscripts or other documentation associated with a dataset as described in NIST S 1801.01.

DIRECTIVE OWNER

Division 602 – Editorial Review Board Chair

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	04/01/14	Katherine Sharpless	Initial draft
Rev. .01	8/3/2016	Dan Cipra	Formatting updates only
Rev. .02	11/4/2016	Katherine Sharpless	Corrected to include delegation of reviews by division chief for consistency with NIST O 1801.00

Review of Software Intended for Publication

NIST S 1801.03
Effective Date: 12/6/2016

PURPOSE

This suborder provides requirements for review of software that will be made publicly available as a stand-alone product.

APPLICABILITY

This suborder applies to all NIST staff, including full- and part-time employees, temporary government employees, and special government employees.

REFERENCES

- [NIST O 1801.00 NIST Review of Fundamental Research Communications](#)
- [NIST O 1005.00 Administrative Committees](#)

DEFINITIONS

In the context of this directive,

- Computer program means a set of instructions, rules, or routines recorded in a form that is capable of causing a computer to perform a specific operation or series of operations.
- Computer software means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer databases or computer software documentation.

Computer software documentation means owner manuals, user manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.¹

REQUIREMENTS

1. The OU in which software is prepared for public release is responsible for the technical quality of the work and associated review, including, as appropriate:
 - effectiveness and efficiency of algorithms that are embedded in the program
 - completeness and effectiveness of comments, if any, in source code available to the user, if any

¹ [48 C.F.R. §252.227-7013](#)

- presence and effectiveness of operating messages related to user inputs, errors, etc.
 - presence and effectiveness of error recovery provisions
 - presence and effectiveness of "user friendly" provisions such as help messages, menu screens, and installation programs
 - completeness and effectiveness of software testing programs
 - completeness and effectiveness of documentation that makes it possible for users to install and operate the software.
2. The NIST Editorial Review Board (ERB) is responsible for editorial review of associated documentation, which must comply with NIST policies for technical publications, including the inclusion of uncertainties and disclaimers where appropriate, as well as the use of SI units. Total documentation that supports the use of NIST software that is made available to the public must include, as appropriate:
- a description of the purpose of the software
 - a description of algorithms, data tables, etc.
 - a statement describing how to obtain the software
 - hardware requirements for the use of the software:
 - system architecture
 - memory and storage
 - peripherals
 - network dependencies
 - specification of applications programs, if required, to access and use database files, spreadsheet files, word processing files, etc.
 - specification of an interpreter or compiler if one is required to use the program code that is provided
 - statement of program tests, testing levels (alpha, beta, acceptance), test results, and other validation-related information; description and results of tests of embedded algorithms, etc.
 - statement of inputs required from the user
 - statement concerning technical support available from NIST with appropriate contact information
 - software installation instructions appropriate for the intended user
 - instructions for the use of the software (if it is not menu-driven appropriately)
 - statement of error messages, if applicable, and error recovery procedures

- the software disclaimer found at <http://www.nist.gov/open/license.cfm> or another suitable disclaimer as approved by the Office of Chief Counsel for NIST.

ROLES AND RESPONSIBILITIES

Authors

- Prepare software and associated documentation that are of high quality, technically accurate, and editorially correct.
- Report the results of their technical work using the International System of Units (SI) and appropriate statements of uncertainty.
- Are responsible for the correctness of software and associated documentation.
- Are responsible for determining whether or not software and associated documentation raise substantive and sensitive policy issues even for projects that have not themselves been designated as sensitive. If there are sensitive or policy issues, staff members shall allow responsible management to review oral or written reports and include NIST Counsel, if appropriate, before making any disclosure of findings or conclusions to sponsors or others outside of NIST.
- Provide reviewers with access to the software via an appropriate medium (e.g., CD, link), coded (“readme”) text files if they exist, and the documentation manuscript for review.

Division Chiefs, Office Directors, and Center Directors

- Are responsible for authorizing release of fundamental research communications in the form of software prepared by staff members who report to them.
- May delegate authority to approve release of fundamental research communications in the form of software prepared by staff members who report to them.

Other Supervisors (e.g., Group Leaders, Program Managers):

- If so delegated, may provide final review and approve the release of fundamental research communications in the form of software that are prepared under their supervision.

Editorial Review Board Readers, Sponsors, and Chair

- Are responsible for review and approval of manuscripts or other documentation associated with software as described in NIST S 1801.01.

DIRECTIVE OWNER

Division 602 – Editorial Review Board Chair

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	04/01/14	Katherine Sharpless	Initial draft
Rev. .01	8/3/2016	Dan Cipra	Formatting updates only
Rev. .02	11/4/2016	Katherine Sharpless	Corrected to include delegation of reviews by division chief for consistency with NIST O 1801.00

Review of Scholarly and Technical Videos Intended for Publication

NIST S 1801.04
Effective Date: 07/26/2016

PURPOSE

This directive describes the requirements for review of videos intended for publication and viewing by a technical audience rather than by the general public.

APPLICABILITY

This suborder applies to all NIST staff, including full- and part-time employees, temporary government employees, and special government employees.

REFERENCES

- [NIST O 1801.00 NIST Review of Fundamental Research Communications](#)
- [NIST O 1005.00 Administrative Committees](#)
- [Editorial Review Board Charter](#)

DEFINITIONS

In the context of this directive, a scholarly or technical video is one in which a demonstration or tutorial is provided.

REQUIREMENTS

1. Videos must comply with NIST policies for fundamental research communications, including the inclusion of measurement uncertainties and disclaimers where appropriate, as well as the use of the SI units. The OU in which a video is prepared is responsible for the quality of the technical content. The OU in which a video is prepared is responsible for reviewing scripts and other materials to ensure that the video complies with NIST policy.
2. The originating OU for a video is the OU of the corresponding or senior NIST author unless there is agreement to a different arrangement. The originating OU has primary responsibility for the quality of the recording as well as the quality of the technical information presented. Review and approval within the originating OU are required to ensure that a video is complete and that revisions necessary to meet NIST quality requirements have been made. Review within the originating OU must thoroughly address technical content, editorial quality, and policy issues.

3. Videos presented to the Editorial Review Board (ERB) must be approved in the Editorial Review System. In every case, the approval of the Division Chief (or equivalent) must be recorded, indicating that the video has been reviewed and approved in the originating OU.¹
4. ERB review consists of review and approval by
 - one or more ERB readers, one of whom must be external to the originating division unless permission to use a division member is approved by the ERB Sponsor, the ERB Chair, or the OU Director,
 - the designated ERB Sponsor, and
 - the ERB Chair.
5. In special cases as described in NIST O 1801.00, additional reviews may be required.
6. For a noting, review and approval by the Division Chief (or equivalent), ERB Sponsor, and ERB Chair are required. Review and approval by an ERB Reader is not necessary. The ERB Reader(s) must not be involved in the technical work, the documentation, or their direct supervision. The ERB Reader(s) may not be from the same division as the video's primary author(s) unless permission is granted by the ERB Sponsor, ERB Chair, or OU Director.

ROLES AND RESPONSIBILITIES

Authors

- Prepare videos that are of high quality, technically accurate, and editorially correct.
- Are responsible for having scripts and other relevant documents reviewed by division management prior to recording the video.
- Report the results of their technical work using the International System of Units (SI) and appropriate statements of uncertainty.
- Are responsible for the correctness of technical results.
- Are responsible for determining whether or not a video raises substantive and sensitive policy issues even for projects that have not themselves been designated as sensitive. If there are sensitive or policy issues, staff members shall provide their Division management and OU Management with oral or written reports and include NIST Counsel if appropriate after consulting with OU management, before making any disclosure of findings or conclusions to sponsors or others outside of NIST.
- Suggest Editorial Review Board readers when submitting a video to ERB via the Editorial Review System (in consultation with co-authors, division chiefs, and others as appropriate). Persons suggested should be technically informed about the subject, objective, and removed from any conflict of interest that might arise from working in the organizational environment(s) of the author(s).

¹ Note that completion and retention of a NIST-114 is no longer required.

OU Management (Directors, Division Chiefs, Group Leaders)

- Review and approve videos, checking for quality of technical content as well as editorial and policy issues.
- Examine videos for consistency with NIST statutory authority and operating policies; appropriateness of selected medium for publication; appropriate recognition of sponsors, institutions, and persons; and other relevant matters.

Editorial Review Board Readers

- Review and approve videos, checking for technical quality as well as editorial and policy issues.
- Provide critical evaluation of the technical content and methodology, statistical treatment of data, uncertainty analysis, use of appropriate reference data and units, and bibliographic references.
- Examine videos for quality and correct use of language, freedom from jargon, clarity of expression, effective organization, good format, appropriate title, adequate references, indexing, citations, footnotes, and figures.
- Are encouraged to communicate directly with authors regarding their comments and suggestions. However, in unusual cases, readers may choose to remain anonymous. In this case, unsigned comments are sent to the video's ERB Sponsor.

Editorial Review Board Sponsors

- Confirm suitability of Editorial Review Board Reader as selected by the author or the author's superior(s).
- Review and approve videos, checking for editorial and policy issues as well as quality of technical content, as applicable. Sponsors' recommendations may include the need for additional technical or management review including recommendations that management request legal review.
- Examine videos for consistency with NIST statutory authority and operating policies; appropriateness of selected medium for publication; appropriate recognition of sponsors, institutions, and persons; and other relevant matters.
- Examine videos for quality and correct use of language, freedom from jargon, clarity of expression, effective organization, good format, appropriate title, adequate references, indexing, citations, footnotes, and figures.
- When necessary, arbitrate differences of opinion between readers and authors, recommend additional readers if required, or take other steps to resolve issues.

Editorial Review Board Chair

- Approves the release of videos intended for publication.

- When necessary, arbitrates differences of opinion between readers and authors, recommends additional readers if required, or takes other steps to resolve issues.

DIRECTIVE OWNER

Division 602 – Editorial Review Board Chair

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	04/01/14	Katherine Sharpless	Initial draft
Rev. .01	8/3/2016	Dan Cipra	Formatting updates only

Facilities and Site Management

NIST P 2100.00
Effective Date: 8/28/2015

PURPOSE

Direct the establishment of a facilities and site management program for the safe, efficient, economical, and sustainable stewardship and protection of real property assets.

SCOPE

This policy applies to all real property assets, owned, leased, or operated by NIST and to all NIST employees and Associates to the extent allowed by law and the terms of the Associate's agreement.

LEGAL AUTHORITY AND REFERENCES

- 15 U.S.C. § 278c - Acquisition of Land for Field Sites - <http://www.gpo.gov/fdsys/pkg/USCODE-2013-title15/pdf/USCODE-2013-title15-chap7-sec278c.pdf>
- 15 U.S.C. § 278d – Construction and Improvement of Buildings and Facilities - <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title15/pdf/USCODE-2010-title15-chap7-sec278d.pdf>
- 15 U.S.C. § 278e(b) - <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap7-sec278e.pdf>
- Executive Order No. 13693 – Planning for Federal Sustainability in the Next Decade, 19 March 2015 - <http://www.gpo.gov/fdsys/pkg/FR-2015-03-25/pdf/2015-07016.pdf>.
- Executive Order No. 13327 – Federal Real Property Asset Management, 4 February 2004 <http://www.gpo.gov/fdsys/pkg/FR-2004-02-06/pdf/04-2773.pdf>
- 41 C.F.R. Part 102-74 - Facility Management – http://www.ecfr.gov/cgi-bin/text-id?SID=9557d2445027ea511798bbdc452b86c0&node=pt41.3.102_674&rgn=div5
- Department of Commerce Real Property Manual, August 2014 and subsequent revision - <http://www.osec.doc.gov/ofeq/Documents/ORPP/doc%20real%20property%20management%20manual%202014%20official%20copy.pdf>

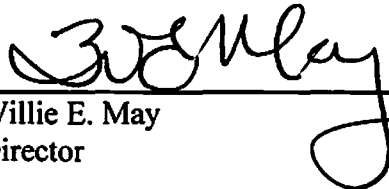
POLICY

It shall be the policy of NIST to establish a comprehensive life-cycle approach to facilities management, including planning, investing, using and divesting of real property assets. (Real property is fixed (unmovable) property, principally land and buildings, and also rights and interests with respect to this property.) The Office of Facilities and Property Management (OFPM) shall provide for:

- Effective and efficient management, maintenance and operations of NIST facilities to preserve these assets consistent with available funding.
- Sustainable design, construction, maintenance, and operation of NIST owned facilities.
- Investment and utilization to realize the best value from real property assets.
- The physical security of NIST assets, facilities and people.

The OFPM serves as the NIST focal point for safely and reliably managing and operating NIST facilities, and providing cost-effective and efficient services and infrastructure programs essential for NIST's operations at all NIST-owned sites, ensuring maximum responsiveness to the needs of NIST's technical programs. NIST Organizational Unit Directors, working with the Chief Facilities Management Officer, shall provide timely information and engagement to develop the strategy to meet their program requirements. The cooperation and engagement of all facility and site occupants is essential in the stewardship of the site as their activities directly impact the cost to maintain and operate the facilities.

The Associate Director for Management Resources shall ensure the development of other directives as necessary for the full and effective implementation of this policy.


Willie E. May
Director

AUG 28 2015
Date

Laboratory and Work Space Decommissioning

NIST PR 2100.01
Effective Date: 3/21/2016

PURPOSE

To provide procedures for evaluating, testing, and decontaminating work spaces, supplies, and property that might be contaminated from process contamination related to laboratory activities or other work activities. Decommissioning is required to ensure that employees, contractors, future tenants of interior building spaces, the general public, and the environment are protected from hazardous chemical, physical, and biological materials, and radioactive material sources that may have resulted from previous laboratory processes or work activities.

Although this directive was developed with a focus upon laboratory activities, this directive applies to all Organizational Units to ensure that all spaces where contamination may exist due to the activities undertaken within are properly cleared or decontaminated upon the cessation of that activity in the space.

APPLICABILITY

The provisions of this procedure apply to all NIST-controlled facilities. They also apply to all property located in labs and other NIST-controlled spaces.

This directive is applicable to all NIST employees and associates engaged in activities involving hazardous materials at or for NIST, to the extent allowed by law and the terms of the associate's agreement.

NIST employees and associates to whom the provisions of this procedure apply are referred to in this procedure as "covered employees and associates."

REFERENCES

- [29 CFR 1926 Subpart T, Demolition](#)
- [10 CFR 20, Subpart E, Standards for Protection Against Radiation](#)
- ANSI/AIHA Z9.11-2008, American National Standard for Laboratory Decommissioning
- [Executive Order 12196, Occupational Safety and Health Programs for Federal Employees](#)
- [Public Law 91-596, \(Williams-Steiger\) Occupational Safety and Health Act of 1970](#)
- [Title 29 CFR Part 1910, Occupational Safety and Health Standards](#)
- [Title 29 CFR Part 1926, Safety and Health Regulations for Construction](#)

- [Title 29 CFR Part 1960, Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters, Subpart I for Recordkeeping and Reporting Requirements](#)
- [United States Nuclear Regulatory Commission Consolidated Guidance About Materials Licenses: Program-Specific Guidance About Academic, Research and Development, and Other Licenses of Limited Scope Including Gas Chromatographs and X-Ray Fluorescence Analyzers \(NUREG-1556, Volume 7\)](#)
- [40 CFR 261.3, Definition of Hazardous Waste](#)
- [Facilities and Site Management, NIST P 2100.00](#) (8/28/2015)
- [NIST S 7101.50 - Biosafety Program](#) (4/1/2014)
- [NIST P 7200.00 - Ionizing Radiation Safety](#) (9/5/2012)
- [NIST O 7201.00 - Ionizing Radiation Safety - Radioactive Material and Ionizing-Radiation-Producing Machines](#), (1/15/2014)
- [Personal Property Management Program Order, 2102.00](#)

DEFINITIONS

Associate – An individual working at but not employed by NIST. [Types of NIST associates](#) include, but are not limited to, foreign and domestic guest researchers, facility users, contractors, and students.

Associated Space – A non-laboratory space, such as an office or storage room, that is used to support the laboratory activities and may have contained bulk hazardous materials or process contamination as a result of the laboratory activities.

Clearance - A radiological assessment of a facility and/or items and equipment to affirm conditions are suitable for unrestricted release. The assessment is coordinated through the Gaithersburg Radiation Safety Division (GRSD) or the Radiation Safety Officer (RSO) in Boulder.

Contamination – The presence of any substance or odor that is potentially harmful, hazardous.

Decommissioning – The formal deactivation of a laboratory and/or associated space, assuring the safety of the space for further cleaning, renovation, or occupancy.

Deployment Tools – Procedures, forms, instructions, user guides, IT applications, and/or training.

Employee – An individual employed by NIST.

Health Hazard – Refers to chemicals for which there is statistically significant evidence based on at least one study conducted in accordance with established scientific principles that acute or chronic health effects may occur in exposed employees. A condition in which an

employee's exposure to a chemical substance, biological agent, or physical agent is in excess of those permitted levels established by the regulatory agencies with jurisdiction, or in excess of guidelines established by consensus standards organizations, or any other generally recognized hazard that affects employee health (e.g., poor sanitation).

Hazardous Materials – Hazardous liquids, gaseous, or solid materials stored in equipment, furnishings, or building systems (fuels, lubricants, refrigerants, etc.), laboratory chemical stores, microbiological materials or biologically active materials, solid radioactive sources, radionuclides, and containerized chemical waste. These materials are not integral to equipment or materials and can be removed and contained.

Hazardous Waste – See definition at 40 CFR 261.3.

Intrinsic Hazardous Materials – Hazardous materials that make up or are included within building materials and/or equipment by design as opposed to contamination. Examples are asbestos, lead paint, mercury, and Polychlorinated Biphenyls (PCBs).

Ionizing Radiation – Sometimes referred to hereafter as “radiation,” alpha particles, beta particles, gamma rays, x rays, neutrons, high-energy electrons, high-energy protons, and other particles capable of producing ions when they impinge on, or penetrate matter.

Ionizing-Radiation-Producing Devices – Devices that generate ionizing radiation when energized, including, but not limited to, X-ray units, particle accelerators, neutron generators, and electron microscopes.

Laboratory Supervisor – The OU management person in charge of a designated lab.

NIST Safety Program – A written document and any associated deployment tools, best practices, and other related resources, that asserts the operational requirements and identifies the individuals responsible for implementing those requirements for a given safety topic with the intent of providing a safe and healthful working environment.

Organizational Unit (OU) – Term used herein to denote any of the following: the Office of the Director, the three Associate Director organizations, the two NIST Centers, the five NIST Laboratories, the three Extramural Programs, and the six Chief Offices.

Office of Facilities and Property Management (OFPM) – The NIST Organization charged with providing, maintaining, and configuring facilities for use.

Organizational Unit (OU)/Division Safety Personnel – Employees, such as OU Safety Coordinators and Division Safety Representatives, who perform designated safety-related duties for their OU or division on a full- or part-time basis.

Principal Investigator (PI) – The lead scientist or engineer or space occupant for a particular well-defined science (or other research) project, such as a laboratory study or clinical trial. It is often used as a synonym for "head of a laboratory space" or "research group leader," not just for a particular study.

Personal Property – Physical property of any kind except Real Property (land, buildings). This includes but is not limited to laboratory furnishings, equipment, tools, and instruments.

Process Contamination – Contamination of a facility, including equipment and furnishings, that has resulted from the processes conducted therein. This includes radioactive, chemical, explosive, and/or biological contamination. This term is limited to materials and quantities declared to be hazardous by federal or state regulations or other applicable standards. It does not include materials used in the construction of the facility, equipment, or furnishings or background constituents that are indigenous.

Radiation Safety Officer (RSO) – The individual, meeting the requirements of the NRC, who is responsible for managing the Radiation Safety Program (RSP), including all aspects of the utilization of sources under the RSP, in accordance with the requirements of NIST's NRC licenses; applicable Federal, State, and local regulations; and this procedure.

Shall/Should/May –

- (1) Shall (Must or Will): Indicates that the performance of an item or portion of a procedure is mandatory.
- (2) Should: Indicates that the performance of an item or portion of a procedure is not mandatory, but the full implications of not performing that item or portion of a procedure must be understood and carefully weighed before choosing a different course.
- (3) May: Indicates that the performance of an item or portion of a procedure can be considered for use, or non-use, at the discretion of the individual responsible for the action.

Supplies - Materials(s) used or created in the Laboratory.

Qualified Safety, Health, and Environmental Professional - The term Safety and Health Specialist means a person or persons meeting the Office of Personnel Management standards for such occupations, which include but are not limited to:

Safety and Occupational Health Manager/Specialist GS-018
Safety Engineer GS-803
Fire prevention Engineer GS-804
Industrial Hygienist GS-690
Fire protection and Prevention Specialist/Marshal GS-081
Health Physicist GS-1306
Occupational Medicine Physician GS-602
Occupational Health Nurse GS-610
Safety Technician GS-019
Physical Science Technician GS-1311
Environmental Health Technician GS-699
Air Safety Specialist GS-1825

Chemist GS-1320

Health Technician GS-645

Highway Safety Manager GS-2125

or equally qualified military, agency, or nongovernment personnel. The agency head shall be responsible for determination and certification of equally qualified personnel.

Workspace Supervisor – The supervisor of the activity occurring within the office, laboratory, storage area, or other interior space. Examples might be a PI, a shop supervisor, or a hazardous waste coordinator.

RESPONSIBILITIES AND AUTHORITIES

OU Directors:

- (1) Establish policies and procedures, as needed, for implementing this procedure within their OUs and ensuring the implementation of those policies and procedures.
- (2) Ensure subordinate managers have the authority, resources, and training needed to implement this procedure.
- (3) Ensure that workspace supervisors properly decommission or perform clearances for each interior space that is vacated or changed in activity.
- (4) Ensure that the OU performs proper recordkeeping (in accordance with NIST – 88 Form, Appendix B) for all workspace decommissioning, and/or clearance activities to include third party verification if required.
- (5) Control possession and/or access to potentially harmful items, equipment, and facility locations and for obtaining evaluation and testing services from the Office of Safety, Health, and Environment (OSHE), or OSHE recommended service provider, on an as needed basis.
- (6) Ensure workspace decommissioning and/or clearance conditions are accepted by OFPM.

Chief Facilities Management Officer (CFMO):

- (1) Ensures that this procedure is integrated effectively into NIST's overall management system.
- (2) Ensures that this procedure is effective, efficient, and continually improved to meet the needs of NIST management, employees, and associates.
- (3) Supervises OFPM staff in the performance of inspections, development of corrective action punch lists, and final determination on the acceptance of workspace conditions as decommissioned and/or cleared, and posting of Construction Notices on doors upon acceptance of transfer.

Occupational Safety Health and Environment (OSHE) Staff:

- (1) Assists OU and OFPM personnel in making decisions on hazardous material exposure limits.
- (2) Makes decisions on releasability of materials, equipment, and areas that have contained hazardous materials.

Division Chiefs (or Equivalents):

- (1) Implement this procedure within their organizations in accordance with the policies and procedures established by their OUs.
- (2) OFPM Safety Group working with OSHE's Gaithersburg Radiation Safety Division (GRSD), Gaithersburg Safety Health and Environment Division (GSHEd), and/or Boulder Safety and Environmental Health Division (BSHEd), as appropriate, are responsible for determining what items, equipment, and facility locations should be tested, what testing methods should be used, and if test results are acceptable.

NOTE: Some NIST OUs do not have Division Chiefs; these OUs shall designate other individuals to carry out these responsibilities.

Workspace Supervisors:

- (1) Ensure workspace decommissioning and/or clearance activities are conducted in accordance with this procedure.
- (2) Fill out and sign the appropriate documentation for workspace decommissioning and/or clearance activities, and submit it to their OU management.

Organizational Unit (OU)/Division Safety Personnel:

- (1) Assist with the implementation of this procedure in accordance with policies and procedures of their OU/division.

Covered Employees and Associates:

- (1) Complete the training designated by their OUs and work in accordance with that training and request additional training as needed or as conditions change.

PROCEDURES

a. Workspace Decommissioning Preplanning

- (1) Decommissioning shall be conducted for every workspace and associated space that is going to be vacated for any of the following reasons:
 - (a) The space is being converted to a different kind of use; or
 - (b) The space is being vacated; or
 - (c) The space is to be renovated or demolished.
- (2) Space owner conducts a review meeting with OSHE and OFPM to discuss the following:
 - (a) Identify area for decommissioning and/or clearance activity.
 - (b) Determine scope of project, e.g., what are contaminants, how will decontamination and/or clearance activity be performed, what is the final level of contamination allowed.
 - (c) Collect historical data (interviews, documentation, etc.). In accordance with [NIST Records Management Policies](#) and when appropriate, contact the NIST Museum

regarding [preservation services](#). All historical data should be attached to the NIST – 88 Form.

- (d) Review data and determine potential contaminants of concern (PCOC).
- (e) Occupants or staff familiar with specific area hazards are responsible for ensuring that the space is a clean area in preparation for subsequent work. These steps may be included in the planning process:
 - 1. Disposal of hazardous wastes (see OSHE for procedure).
 - 2. Disposal of hazardous materials (see OSHE for procedure).
 - 3. Decontamination and removal of experimental equipment (see OSHE for procedure).
 - 4. General cleaning of work surfaces using soap and water or materials appropriate to the agents in use.
 - 5. Final survey with Qualified Safety Health & Environment professionals to determine removal of general hazards.

b. Workspace Decommissioning

- (1) The workspace supervisor shall be responsible for decommissioning their space and leaving the space in a safe condition for further cleaning, renovation, demolition, or occupancy. All chemical, biological, and radiological materials, all contaminated pieces of equipment, all physical hazards such as needles, all process contamination, and all other waste materials shall be removed or decontaminated from the workspace.

(2) Chemicals

- (a) The workspace supervisor shall remove all chemicals, including compressed gas cylinders and cryogens, specimens or materials, from the space, prior to vacating, unless the project continues under another workspace supervisor. Useable chemicals shall be transferred to another workspace supervisor or to the OFPM/Facilities Services Division (FSD) Storeroom. Waste chemicals shall be disposed of by following the standard procedure to request a chemical waste pickup through OSHE.
- (b) Gas cylinders or dewars shall be returned to supplier or OFPM/FSD storeroom.

(3) Biological Agents

- (a) The workspace supervisor that is responsible for decommissioning and or clearance of a space that contains or has contained biological agents shall contact the site Biosafety Officer (BSO) for direction per NIST Biosafety Program Suborder, [NIST S 7101.50](#).
- (b) The decommissioning of a space that contains or has contained biological agents shall be performed in accordance with the [NIST Biosafety Program](#).

(4) Radioactive Material or Ionizing Radiation Sources

- (a) The workspace supervisor that is responsible for decommissioning and/or clearance of a space that contains or has contained radioactive materials or ionizing-radiation-producing devices shall contact the site RSO for direction.
- (b) The decommissioning and/or clearance of a space that contains or has contained radioactive materials or ionizing-radiation-producing devices shall be performed in accordance with the NIST Ionizing Radiation Program, and the applicable Nuclear Regulating Commission (NRC) license
- (c) See references below:
 - i. [Policy 7200.00 Ionizing Radiation Safety](#); and
 - ii. [Order 7201.00 - Ionizing Radiation Safety - Radioactive Material and Ionizing-Radiation-Producing Machines](#); and
 - iii. Ionizing Radiation Safety Committee (IRSC) Home Page.

c. Decontamination of Surfaces and Items

- (1) If any activities in the space may have resulted in process contamination, all fixed potentially-contaminated surfaces and items shall be decontaminated. All potentially-contaminated moveable items shall be tested and/or decontaminated before they are removed from the space.
- (2) Chemicals and materials that may leave residual process contamination include, but are not limited to, the following:
 - (a) Asbestos;
 - (b) Metals and heavy metal compounds;
 - (c) Polychlorinated biphenyls;
 - (d) Dioxins;
 - (e) Pesticides;
 - (f) Perchloric acid, particularly in fume hood vents;
 - (g) Engineered nanomaterials;
 - (h) Heavy metal azides in sanitary plumbing;
 - (i) Reactive/energetic compounds, such as organic peroxides, hydrides, azides, and picric acid; and
 - (j) Radiation

- (3) Decontamination of space surfaces or equipment may produce hazardous waste, especially if contaminated with D- or P-listed hazardous wastes (261.30, 33). Contaminated wash water may not be discharged to the sanitary sewer or to storm water.
- (4) The workspace supervisor is responsible to ensure testing has been performed to determine if significant process contamination is present. Sampling should be done in accordance with recognized industrial hygiene or environmental testing procedures, such as Department of Energy (DOE), Environmental Protection Agency (EPA), National Institute of Occupational Safety and Health (NIOSH) or Occupational Safety and Health Administration (OSHA) sampling and analytical methods.
- (5) Appendix A of this procedure lists surface contamination levels that are acceptable to NIST, which have been calculated using the method from ANSI/AIHA Z9.11-2008 and occupant exposure limits (OELs) that are current as of 2012. Appendix B of ANSI/AIHA Z9.11-2008 uses the ratio of the beryllium surface contamination standard and its permissible exposure limit (PEL) to calculate surface contamination standards for other metals based on their OELs.
- (6) If a potentially-contaminated surface or item is not tested for contamination, the surface or item shall be assumed to be significantly contaminated.
- (7) If a piece of property is shown or assumed to have an unacceptable level of contamination it must be decontaminated and retested. This shall be repeated until the sampling shows the level of contamination to be below the applicable release criteria.
- (a) If a piece of property contains an intrinsic hazardous material, such as asbestos-containing components, used oil, PCBs, refrigerants, or batteries, the PI/supervisor shall contact the OFPM FSD Property Office and/or OSHE to determine the proper manner of handling the property.
- (b) Personal property found to be contaminated and not able to be cleaned sufficiently for reutilization or standard disposal processes must be disposed of by a qualified commercial firm. In this case, the lab shall complete the [NIST-5 Form](#) in detail. Prior to moving the equipment from the contaminated area, lab personnel will advise the FSD or the BMSS Division Property Group of the nature of the contamination, in order that the Property Group can coordinate pick up between the lab and the qualified disposal activity. Each Property Custodian responsible for equipment in the area being decommissioned will create a [NIST-5 Form](#), and upon pick up by the contractor, will ensure that the contractor has signed for the equipment. The Property Custodian is responsible for ensuring that the contractor removes all NIST markings prior to turning over the equipment to the contractor.
- (c) Property Custodians with equipment affected by the decommissioning will create a [NIST-6A Form](#) and forward it, with the [NIST-5 Form](#), to the FSD or BMSS Property Group, for coordination with the Property Board of Review

<https://inet.nist.gov/forms/upload/n6apo.pdf>). Once approved by the Property Management Officer, the items may be administratively removed from the inventory, using a voucher number for identification.

All workspace equipment that is to be excessed through OFPM Property Control requires a NIST-5 certification form to accompany the equipment.

d. General Cleaning

- (1) All storage equipment, including but not limited to storage cabinets, refrigerators and freezers, centrifuges, cryostats, and fume hoods, shall be emptied and cleaned.
- (2) All surfaces within the workspace and associated areas shall be cleaned with soapy water, or the equivalent, prior to vacating the lab.
- (3) All paper, rags, empty bottles, boxes, glassware, plasticware, etc. are to be properly disposed prior to vacating the lab.
- (4) Cleaning of a workspace that has undergone a clearance can commence with cleaning provided Radiation Safety has approved the area for unrestricted release.

e. Documentation of Decommissioning

- (1) The OU shall maintain records of all workspace decommissioning and forward a copy to OFPM Safety Group.
- (2) The workspace supervisor shall complete and sign the NIST-88 Form <https://inet.nist.gov/forms/upload/n6apo.pdf> and submit it to their OU and OFPM Safety if turning a space over to refurbishment/remodeling by OFPM.
- (3) A representative of the Division or OU shall also sign the completed form. This representative can be the Division Chief or OU Director.
- (4) The OU shall maintain all workspace decommissioning records for the life of the building plus 30 years. Documentation shall be kept as Occupational Health and Safety Building Area Monitoring, Testing, and Exposure Level Compliance Records.
- (5) Upon acceptance of the decommissioning or clearance, OFPM will retain a copy of the forms as part of the permanent building records.

DIRECTIVE OWNER

190.00 – Chief Facilities Management Officer

APPENDICES

- Appendix A. Acceptable Surface Contamination Levels for Selected Hazardous Chemicals
- Appendix B. NIST Laboratory Decommissioning Form
- Appendix C. Revision History

APPENDIX A

ACCEPTABLE SURFACE CONTAMINATION LEVELS FOR SELECTED HAZARDOUS CHEMICALS

Compound	Acceptable Surface Contamination Level ($\mu\text{g}/100\text{ cm}^2$)		Source	Occupational Exposure Limit ($\mu\text{g}/\text{m}^3$)
	Laboratory or Operational Area	Non-Laboratory or General Public		
Arsenic	15	1	Be Ratio*	10 [†]
Beryllium	3	0.2	DoE 10 CFR 850.30-31	2 [‡]
Cadmium	7.5	0.5	Be Ratio*	5 [‡]
Chromium III	750	50	Be Ratio*	500 ^{†‡}
Chromium VI	7.5	0.5	Be Ratio*	5 [‡]
Cobalt	30	2	Be Ratio*	20 [†]
Lead	26.9	4.3	EPA/HUD Regs. Interior window sills / Floors	50 ^{†‡}
Manganese	300	20	Be Ratio*	200 [†]
Mercury	37.5	2.5	Be Ratio*	25 [†]
Nickel	1500	100	Be Ratio*	1000 [‡]
Silver	15	1	Be Ratio*	10 [‡]
PCB	100	10	EPA TSCA Regs.	-

* – Per the method used in ANSI/AIHA Z9.11-2008

[†] - American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Value (TLV)

[‡] - Occupational Safety and Health Administration (OSHA) Permissible Exposure Limit (PEL)

APPENDIX B

NIST LABORATORY DECOMMISSIONING DOCUMENTATION FORM

NIST-88 (4-2015) NIST PR 2101.01	U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
LABORATORY DECOMMISSIONING DOCUMENTATION FORM	
The Principal Investigator or Lab Supervisor shall complete this form for any laboratory and/or associated space that is being vacated or decommissioned. This form shall be submitted to the Operating Unit for recordkeeping.	
PI/Lab Supv: _____ Date: _____	
OU: _____ Division: _____ Room: _____	
Lab Name & Use: _____	
HAZARDOUS MATERIALS & LABORATORY EQUIPMENT	
Y N NA <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Hazardous materials (chemical, biological, radioactive) removed from area, including storage cabinets, etc. <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Hazardous materials removed from associated spaces (e.g. refrigerators, storage rooms) <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Compressed gas cylinders returned to vendor, transferred, or disposed as waste <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Hazardous waste disposed of through normal hazardous waste pickup procedure <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> All glassware, equipment, apparatus, etc. removed from area <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> All accessible surfaces cleaned and all trash properly disposed of	
LIST POTENTIAL PROCESS CONTAMINANTS: (before cleaning / decontamination)	
Chemical _____ Biological* _____ Radioactive** _____ No Hazard _____	
<small>* Property used with biological materials requires clearance by the Biosafety Officer. ** Property used with radioactive materials or X-ray equipment requires clearance by the Radiation Safety Officer.</small>	
LIST POTENTIAL PROCESS INTRINSIC HAZARDOUS MATERIALS: (before cleaning / decontamination)	
Asbestos _____ Batteries _____ Liquids _____ PCBs _____	
Other _____	
SAMPLING FOR POTENTIAL CONTAMINANTS:	
Analyte _____	Method _____
Results _____	Clearance Criteria _____
Analyte _____	Method _____
Results _____	Clearance Criteria _____
PROCEDURES USED FOR CLEANING/DECONTAMINATING SURFACES AND EQUIPMENT:	
_____ _____ _____	
To the best of my knowledge, this laboratory and associated spaces have been decommissioned in accordance with NIST Policy.	
Principal Investigator/Lab Supervisor (signature) _____	Date _____
Division or OU Representative (signature) _____	Date _____
<small>Forms Repository</small>	

[Reset Entire Form](#)

[Print Form](#)

APPENDIX C

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	3-12-2015	Rich Royer	New Draft
Rev .01	10/23/2015	Dan Cipra	Formatting changes
Rev. .02	2/10/2016	Virginia Holtzman-Bell	Incorporated changes from DRB
Rev. .03	3/10/2016	Dan Cipra	Formatting updates

Personal Property Management Program

NIST O 2102.00
Effective Date: 4/16/2015

PURPOSE

This document establishes requirements and responsibilities for the management of accountable property, i.e., personal property and precious metals.

APPLICABILITY

This Order is applicable to all NIST Employees and End Users.

REFERENCES

- [The Federal Property and Administrative Services Act of 1949](#), 40 USC 482, et seq.
- [Federal Management Regulation \(FMR\) 41-CFR-102](#)
- [Federal Property Management Regulations \(FPMR\) 41 CFR 101](#)
- [Public Law 102-245](#) American Technology Preeminence Act of 1991
- [Public Law 95-224](#) Federal Grant and Cooperative Agreement Act of 1977
- [Federal Acquisition Regulation 52.245-1](#)
- [Executive Order 12999](#) Educational Technology: Ensuring Opportunity for All Children in the Next Century
- [Department Administrative Order 200-0](#) Department of Commerce Handbooks and Manuals
- [Department Personal Property Management Manual \(PPMM\)](#)

DEFINITIONS

Accountable Personal Property - Property for which accountability must be maintained in the NIST Personal Property Management System. Accountability must be maintained for;

- Any tangible asset with a unit cost of \$5,000 or greater and that does not lose its individuality while fulfilling its function. As an example, an air conditioning unit purchased at a cost of \$6,000 that is permanently installed in a facility is, for this purpose, said to have lost its individuality and is not tracked as a personal property asset. A portable air conditioning unit however, purchased at the same cost as the permanent unit and used to augment cooling when an installed unit fails, remains a personal property asset as it retains its individuality while fulfilling its function;
- Precious metals;

- Personal property with an acquisition cost less than \$5,000 that may be converted to private use or has a high potential for theft and listed as a personal appeal item;
- All personal property loaned or leased to NIST and planned to remain on site for 90 days or longer;
- All government-furnished accountable property, which includes government-owned property in the possession of or directly acquired by the government and subsequently made available to a contractor. Government-furnished property also includes contractor-acquired property that at the end of the contract will remain government property and
- All Contractor or Grantee personal property, which includes property owned by a contractor or grantee that remains as property of the contractor or grantee when the contract or project is completed. This property shall be labeled with information indicating ownership, e.g., contractor or Grantee Company name, to minimize confusion for accountability of NIST property.

End User - Any employee, affiliate, contractor or associate who uses, supervises the use of, or has control over government property.

Fabricated Asset – A tangible asset manufactured in the course of NIST research and owned by NIST with a life expectancy of more than one year.

Heritage Asset – Personal property that is retained for its historic, cultural, educational, scientific, artistic or other intangible value as opposed to its current usefulness is carrying out the NIST mission.

Personal Appeal Asset: Any item that by its inherent nature is deemed particularly susceptible to conversion to personal use.

Personal Property – Property of any kind except real property (land, buildings), intellectual property and records of the federal government, including consumable supplies and tangible assets not meeting the definition of accountable personal property.

Personal Property Management System: That set of software and data bases within which the NIST accountable property records are maintained.

Precious Metal – Any metal or metal alloy having a high monetary value in relation to its volume or weight and without regard to form.

Property Board of Review (PBR) - A standing committee appointed by the Property Management Officer (PMO), typically consisting of five to six members otherwise assigned as Senior Management Advisors or Administrative Officers. The PBR examines the facts of cases of unaccounted property referred to it, so as to determine and establish the extent of personal liability for lost or damaged property. The PBR makes recommendations to the PMO regarding the removal of items from official property records. The PBR has the authority to perform an inquiry of reported property losses, as deemed warranted and to request verbal presentations to

the PBR by appropriate NIST employees, in order to fully understand the circumstances leading to the lost property.

Property Official (PO) - Any individual with defined property responsibilities:

- Property Management Officer (PMO);
- Property Accountability Officer (PAO);
- Property Custodian (PC);
- Division Chief (DC);
- Supervisors and
- Users.

Real Property - Any property attached directly to land, as well as the land itself. Real property not only includes buildings and other structures, but also rights and interests.

Secured – Maintained in such a manner as to prevent damage, loss or theft.

REQUIREMENTS FOR MANAGEMENT OF PERSONAL PROPERTY

- Accountable property shall be secured and used only in accordance with governing laws, regulations and policies.;
- Accountable property shall be procured, received, tracked and inventoried in accordance with documented procedures;
- Accountable property transactions shall be processed on the required forms and recorded in the appropriate tracking system in a timely manner, i.e., property management;
- Proper procedures shall be followed to retire property;
- Lost, stolen or missing property shall be promptly reported and processed through a regularly conducted Property Board of Review (PBR) meeting and.
- Property officials shall be trained on their assigned responsibilities.

REQUIREMENTS FOR EMPLOYEE TRAINING

In general, all employees will be introduced to the primary concepts of property management as part of the new employee orientation program. The following link lists training requirements http://www.pps.noaa.gov/training_and_education/property-official-certification-program-handbook.pdf. Other training will occur as follows;

- Property Custodians will be provided with the Basic Property Management Training class within 30 business days of having been appointed as a Property Custodian;
- Refresher training for Property Custodians will occur annually and is mandatory;
- Property Custodians will be selectively provided with advanced property management training, as conditions warrant, to include training in
 - Property Disposal Techniques;

- Disposal of Federal Electronic Assets and
- Heritage Asset Management.

REQUIREMENTS FOR MANAGEMENT OF PRECIOUS METALS

- Precious metals must be kept in a secured safe or cabinet locked by a combination lock;
- Precious metals not in use must be secured by the responsible precious metals custodian or designee. Only authorized personnel may have access to the precious metals inventory;
- Precious metal security thresholds limits and record keeping instructions are published in [Administrative Manual Subchapter 7.09](#) Precious Metals;
- Like all other personal property assets, requests for the acquisition of new quantities of precious metals shall not be undertaken without first querying holders of existing inventory as to whether such materials might be available for intra-NIST transfer;
- Precious metal with a value of \$25,000 or greater must be contained in a General Services Administration (GSA) class 5 security cabinet and connected to the NIST security alarm system with restricted access;
- Emergency temporary storage is provided by the Emergency Services Division or the Police Services Group in Boulder. This secure storage is a temporary solution for a period not to exceed 72 hours after which the material must be properly secured in a permanent storage facility, and.
- Precious metals forms must be utilized in managing these assets and are located at the NIST internal forms repository website and include:
 - NIST-1046 (Physical Inventory for Precious Metals),
(<http://inet.nist.gov/forms/upload/n1046.pdf>)
 - NIST-1047 (Current Year Precious Metals Acquisitions),
(<http://inet.nist.gov/forms/upload/n1047.pdf>)
 - NIST-1048 (Current Year Precious Metals Found),
(<http://inet.nist.gov/forms/upload/n1048.pdf>)
 - NIST-1049 (Intra-Office Precious Metals Transfer),
(<http://inet.nist.gov/forms/upload/n1049.pdf>)
 - NIST-1050 (Receipt for Issued Precious Metal),
(<http://inet.nist.gov/forms/upload/n1050-2.pdf>)
 - NIST-1051 (Receipt for Unused Precious Metal), NIST-1052 (Precious Metals Reclassification). (<http://inet.nist.gov/forms/upload/n1051.pdf>)

DELEGATION OF AUTHORITIES

The following authorities were delegated to the NIST Director from the DoC Chief Financial Officer and Assistant Secretary for Administration:

- Designating the Operating Unit Property Management Officer (PMO). Each Operating Unit shall have only one PMO. Neither the title designation nor the responsibilities of the PMO shall be re-delegated. For NIST, the Chief of the Office of Facilities and Property Management Facilities Services Division is designated as the PMO for NIST Gaithersburg and Boulder;
- Authorizing exceptions for replacement standards for office machines, furniture, furnishings and other related equipment specified in FPMR 101-25.301 and 101-25.401;
- Authorizing for official use the retention of abandoned or other unclaimed personal property including voluntarily abandoned or forfeited property;
- Determining and reporting excess personal property to GSA;
- Assigning or transferring excess personal property within the Department, to other federal agencies, to wholly-owned or mixed-ownership government corporations, to cost-reimbursable contractors, or to authorized financial assistance recipients;
- Authorizing transfer of title to government-furnished personal property to contractors or financial assistance recipients in accordance with Public Law 102-245, Public Law 95-224 Section 7(b) (the Federal Grant and Cooperative Agreement Act of 1977), and FAR 52.245-1; and
- Authorizing donation of educationally useful excess personal property to schools or non-profit educational organizations.

RESPONSIBILITIES FOR PERSONAL PROPERTY OFFICIALS

NIST Director is responsible for establishing and administering a Personal Property Management Program within NIST that provides for:

- Creating and maintaining complete and accurate inventory control and accountability records;
- Providing for the proper care and security of personal property including storage, handling and maintenance;
- Identifying personal property no longer required by NIST and making it available for transfer to other DoC activities;
- Ensuring that excess personal property is reported to GSA for transfer, donation, or disposal, as appropriate, under the provisions of the FPMR and PPMM;

- Ensuring that educationally useful excess personal property is made available for donation to schools or non-profit educational organizations in accordance with regulations;
- Submitting required personal property management reports;
- Ensuring that all accountable personal property is maintained in an accurate and timely manner in the NIST personal property management system;
- Informing employees of their responsibilities for government personal property and providing training as needed; and
- Supporting general ledger control accounts for personal property by maintaining appropriate subsidiary accounts and records.

NIST Property Management Officer (PMO) is responsible for the operation of the NIST Personal Property Management Program and is authorized to coordinate the planning and utilization of personal property for the effective and economical accomplishment of operational and mission requirements. The PMO's responsibilities include:

- Providing direction, leadership, guidance and policy in the proper acquisition, accounting, utilization, care and disposal of property;
- Reviewing Organizational Unit (OU) supplemental instructions and guidance on matters of personal property management, so as to ensure consistent compatibility with this Order;
- Evaluating the Personal Property Management Program on a regular basis and determining whether sufficient Property Custodians are in place to programmatically manage accountable property in accordance with governing regulations. The PMO may require a Division to provide an additional custodian, should it appear property related workload is too burdensome for the original number of Property Custodians and other process changes have not been successful in correcting the process deficiency.
- Establishing and maintaining NIST regulations, policies and procedures satisfying the requirements of the Department's PPMM and the various laws, Executive Orders and regulations referenced therein, e.g.:
 - Implementing procedures for the repair and rehabilitation of personal property
 - Providing PAOs with disposition instructions
 - Ensuring that lost, stolen, destroyed, or damaged personal property is investigated
- Ensuring the establishment, training and maintenance of the property management network comprised of Property Accountability Officers Property Custodians, Property Board of Review Members, Division Chiefs and all NIST End Users utilizing personal property;
- Appointing Property Custodians after receiving and concurring with recommendations from the appropriate Division Chief;

- Developing and implementing inventory schedules, monitoring inventory progress and reconciling accountable personal property records with the financial accounting system;
- Delegating, in writing, PAOs to account for and control personal property per the procedures and requirements described herein, (PAO within their assigned jurisdiction;
- Ensuring that excess personal property is archived as “retired” in the NIST personal property management system after final disposition of the property, and.
- Receiving recommendations for the Property Board of Review and making final determinations of the retirement of PRB reviewed assets.

Property Accountability Officer is responsible for coordination and administration of the property management within his or her assigned organization. One PAO is appointed for each campus and provides personal property management guidance to that site and associated remote sites. These responsibilities include:

- Ensuring the effective administration and maintenance of accountability for personal property assigned to their accountability area;
- Ensuring that sufficient Property Custodians are appointed within the organization so as to enable the effective and efficient management of the Personal Property Management Program, and for training newly appointed Property Custodians within 30 days of appointment by the Division Chief;
- Alerting the PMO when PC losses through either transition or attrition result in insufficient PCs;
- Ensuring that PCs have current records for assigned accountable personal property;
- Ensuring that physical inventories are taken, records are reconciled and discrepancies are investigated and resolved in accordance with assigned schedules;
- Ensuring that requests for Property Board of Review actions for lost, stolen, damaged, or destroyed personal property are correctly prepared and processed using form NIST-6A, “Request for Property Board of Review Action;”
- Coordinating actions required by the Property Board of Review;
- Ensuring that personal property is fully utilized, safeguarded from misuse or theft and that unneeded personal property is promptly reported for reutilization, redistribution, or disposal;
- Ensuring that bar code labels are affixed on accountable personal property; and
- Ensuring that receipts, transfers and retirements are accurately and completely entered into the personal property management system in a timely manner.

Property Custodian is responsible for maintaining accountability of all personal property within their assigned area, including:

- Maintaining current custodial records for all accountable personal property, including, but not limited to, maintaining accurate contact and location information in the personal property management system and maintaining records on all loans;
- Initiating documentation as required on all actions affecting the accountability or custody of accountable personal property forms:
 - NIST-6 (Report of Excess Property), (<http://inet.nist.gov/forms/upload/n6po.pdf>)
 - NIST-81 (Intra-Office Transfer of Equipment), (<http://inet.nist.gov/forms/upload/n81po.pdf>)
 - NIST- 6A (Request for Property Board of Review Action), (<http://inet.nist.gov/forms/upload/n6apo.pdf>)
 - NIST 9 (Property Exchange or Return to Sponsor) (<http://inet.nist.gov/forms/upload/n9.pdf>)
 - NIST-393 (Equipment Loan Authorization, Receipt and Property Pass), (<http://inet.nist.gov/forms/upload/n393po.pdf>)
 - And the system provided Business Objects Report PR 003, provided on demand;
- Ensuring that personal property is secured, protected and is used only in accordance with governing laws, regulations and policies;
- Identifying and reporting excess personal property by submitting form NIST-6, “Report of Excess Property” to the PAO;
- Promptly submitting form NIST-6A, “Request for Property Board of Review Action,” for lost, stolen, damaged, or destroyed personal property;
- Conducting annual inventories as required;
- Performing Separation and Clearance Certificate (form CD-126 and NIST-528, “Separation Clearance Certificate”) checks for personal property and reassigning returned and available property as required;
- Ensuring that the personal property management system is updated to reflect the changes if the physical location and/or property contact of accountable personal property changes within a division or OU, and
- Completing the required training.

Organizational Unit Property Point of Contact serves as the senior Point of Contact in each OU and assists the PMO in ensuring the performance of the Property organization within that OU is at an appropriate level. This individual must be either the Senior Management Advisor to the OU Head or the senior Executive Officer in the OU.

Division Chiefs, and/or their organizational equivalents, are responsible for providing management oversight within the property management program within their division, including:

- Monitoring the performance of assigned PCs and ensuring that such personnel are executing their assigned duties in an effective and efficient manner. Recommends personnel for the PC role and identifies replacement PCs to the PMO within ten business days of a vacancy;
- Receiving reports from the assigned PC as to the timeliness of excess and disposal reporting, loan expiration status and inventory reconciliation;
- Ensuring assigned staff are executing their inherent responsibility to safeguard government owned property, that fraud, waste and abuse of government property in their division is not tolerated and for ensuring that information necessary to the adjudication of PBR matters is made available in a timely manner and;
- For reporting losses and corrective measures to the OU head in a timely fashion, and
- For ensuring that property is not disassembled to the piece part level for further use without the express authorization of the Property Management Officer.

Supervisors are responsible for

- Establishing and enforcing administrative and security measures necessary to ensure proper protection and use of all government property under their jurisdiction;
- Ensuring that accountability methods are in place for personal property assets that fall under the \$5,000 accountability threshold or are part of the [NIST appeal list](#);
- Notifying the PC when personal property assets become excess;
- Notifying the PC when personal property assets are Lost, Missing, Stolen, Damaged and Destroyed ;
- Assigning staff to assist the PC in conducting physical inventories in a timely and accurate manner, and
- Ensuring that personal property assets, to include excess and surplus property, are only acquired for government use in accordance with governing laws, regulations and policies..

End User: Each employee, affiliate, contractor or associate who uses, supervises the use of, or has control over government property, is responsible for that property, including;

- Properly caring for, handling, using and protecting government property issued to or assigned for end user use at or away from the office or station;
- Ensuring the proper use, care and protection of all personal property assets in their possession, custody, or control;
- Ensuring that personal property assets in their possession, custody, or control are used only in accordance with governing laws, regulations and policies.;

- Notifying the Property Custodian when an asset's record location is changed for a period in excess of 24 hours;
- Notifying the Supervisor when an asset is no longer required and may be available for reutilization;
- Reporting immediately to Police, their supervisor and their PC any personal property that is Lost, Missing, Stolen, Damaged and Destroyed , and
- Notifying NIST ITAC immediately if the missing property is an IT asset, so as to ensure security and privacy concerns are investigated, necessary follow-up actions are taken (e.g. a remote wipe is sent to a stolen mobile device), and the incident is reported to DOC.

DIRECTIVE OWNER

190 - Director, Office of Facilities and Property Management

APPENDICES

Appendix A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/4/2014	Jack Sweeney	First Draft
Rev. .01	2/18/2015	Jack Sweeney	Updated based on DRB Comments

Facilities and Site Management

NIST O 2103.00
Effective Date: 4/20/2016

PURPOSE

The National Institute of Standards and Technology (NIST) is committed to the efficient and economical use of its real property assets. This order establishes the requirements and associated roles and responsibilities for life-cycle management of NIST facilities as defined within the Department of Commerce (DOC) Real Property Management Manual. Suborders under this order provide more information on responsibilities for specific programs.

APPLICABILITY

In addition to the Office of Facilities and Property Management (OFPM), this order is applicable to all NIST Organizational Units (OUs) and NIST-controlled real property.

REFERENCES

- [15 U.S.C. § 278c - Acquisition of Land for Field Sites](#)
- [15 U.S.C. § 278d – Construction and Improvement of Buildings and Facilities](#)
- [15 U.S.C. § 278e\(b\) - Functions and Activities](#)
- [Executive Order No. 13693 – Planning for Federal Sustainability in the Next Decade](#)
- [Executive Order No. 13327 – Federal Real Property Asset Management](#)
- [41 C.F.R. Part 102-74 - Facility Management](#)
- [Department of Commerce \(DOC\) Real Property Management Manual, August 2014 and subsequent revision](#)
- [DOC Department Organization Order, DOO 30-2B – NIST Organization](#)
- [P 2100.00 NIST Facilities and Site Management](#)
- [OFPM Customer Council Charter](#)

AUTHORITY

The Secretary of Commerce is authorized, under specific conditions (15 USC §278d) and within the limits of funds that are appropriated for NIST, to undertake construction of buildings and other facilities and to make such improvements to existing buildings, grounds, and other facilities occupied or used by NIST as are necessary for the proper and efficient conduct of its activities. The Secretary has delegated this authority to the NIST Director, who has delegated this authority to the Chief Facilities Management Officer (CFMO).

DEFINITIONS

Facilities and Site Management (FSM) –All activities undertaken by OFPM for the life-cycle management of NIST-controlled real property assets, including the providing of facilities related services.

NIST-Controlled Real Property Assets – NIST owned or NIST leased real property, Class 1 (land) and Class 2 (buildings and structures).

NIST Staff – for the purpose of this order and directives developed to implement it, NIST staff refers to Federal employees and associates who are assigned to occupiable space within NIST-controlled real property assets.

Programmatic – Refers to project-related (or task-related) maintenance, modifications, or improvements which are essential to the performance of a particular project (or task) within an OU or division.

REQUIREMENTS

- NIST shall comply with all applicable real property laws, regulations, executive orders, policies and procedures.
- NIST shall implement the DOC real property policies and procedures through the development of supplemental internal NIST-specific real property policies and procedures.
- NIST shall maintain records of all real property under NIST's area of responsibility, such as all documents pertaining to the acquisition, management, and disposal of a real property asset.
- NIST shall ensure that it has the authority to undertake proposed projects and have funds for that purpose.

RESPONSIBILITIES

The NIST Director shall:

- Ensure the development, implementation, maintenance, and continual improvement of the NIST FSM program in accordance with all applicable real property laws, regulations, executive orders, policies, and procedures; and implement the DOC real property policies and procedures.
- Define the roles, responsibilities, and accountabilities and delegate authorities to facilitate an effective FSM program.
- Ensure the availability of resources essential to develop, implement, maintain, and continually improve the FSM program at all operational levels.
- Provide strategic direction and oversight as necessary on significant issues involving FSM stewardship and regulatory compliance.

- Ensure the implementation of accountability and enforcement policies in support of FSM stewardship and regulatory compliance efforts.
- Approve the NIST OFPM Customer Council charter.

The Associate Director for Management Resources (ADMR) (in addition to the responsibilities below for all NIST Associate Directors) shall:

- Ensure the development of the suborders, other directives, and deployment tools necessary for the full and effective implementation of [NIST P 2100.00](#) and this order.

The Chief Facilities Management Officer (CFMO) shall:

- Safely and reliably manage and operate all NIST owned, leased, and operated facilities.
- Provide cost-effective and efficient services and infrastructure programs essential for NIST's operations at all sites, and ensure maximum responsiveness to the needs of NIST's technical programs.
- Set the strategic direction, determine objectives, establish policy, set standards, and propose programming and funding for FSM programs.
- Ensure safety and risk management are integrated in all facilities operations.
- Monitor the condition of NIST real property assets and keep them in good condition. Develop and propose strategies to the NIST Director for real property capital asset management to achieve the aforementioned responsibility.
- Develop, promulgate, and assure compliance of NIST internal directives and procedures to ensure NIST's compliance with all applicable real property laws, regulations, executive orders, policies, and procedures; and implement the DOC real property policies and procedures.
- Manage the OFPM organization and its resources to achieve the goals of this program.
- Chair the OFPM Customer Council.

NIST Associate Directors (as individuals) shall:

- Perform the responsibilities specified for them within individual suborders.
- Consult with OFPM during the development of long range plans, business plans and program requirements to ensure that the facilities requirements are included in their plans.

OU Directors shall:

- Perform the responsibilities specified for them within individual suborders.
- Assist the NIST Director and Associate Directors in carrying out their responsibilities.
- Ensure that staff do not make improvements or modifications to facilities without the prior approval of the CFMO.
- Partner with the CFMO to develop fact-based facilities requirements and recommendations for resource prioritization.
- Be responsible for the increases in staff or operating costs associated with any approved improvement or modification project. The OU will reimburse OFPM for the costs when

OFPM supplies the service associated with the increased demand created by the new programs.

- Be responsible for all costs associated with the operation, maintenance, modification, and improvement of programmatic equipment or systems installed in or attached to NIST facilities.
- Ensure that the employees in their OU participate, as appropriate, in the development, deployment, and maintenance of NIST's FSM program, projects, and plans.
- Ensure all OU staff are compliant with all requirements under this order and associated suborders and procedures.

OFPM Program Managers shall:

- Develop, deploy, and maintain their assigned programs to meet the requirements of this order.
- Carry out responsibilities specific to their assigned programs.
- Serve as the primary point of contact and subject matter expert for their assigned programs.
- Ensure effective communication with all levels of management and staff on program-related issues assigned to them.

The OFPM Customer Council shall:

- Advise the CFMO and serve as the administrative committee reviewing OFPM generated directives, including suborders and procedures.

NIST Managers and Supervisors shall:

- Ensure staff are compliant with all requirement under this order and associated suborders and procedures.

NIST Staff shall:

- Comply with all requirements under this order and associated suborders and procedures, and with additional applicable requirements established by their OU.

DIRECTIVE OWNER

190 – Chief Facilities Management Officer

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	2 Feb 16	Steve Willett (OFPM)	First Draft
Rev. .01	3 Feb 16	Dan Cipra (M&O)	Formatting Updates Only
Rev. .02	4/12/2016	John Bollinger	Incorporated DRB Comments

Acquisition and Disposal of Real Property

NIST S 2103.05

Issue Date: 3/23/2016

Effective Date: 3/23/2016

PURPOSE

To provide guidance on the responsibilities and procedures for the acquisition and disposal of real property assets (i.e., Class 1 land and/or Class 2 buildings/structures) in support of the National Institute of Standards and Technology (NIST) mission.

APPLICABILITY

In addition to the Office of Facilities and Property Management (OFPM), this order applies to all NIST Organizational Unit (OU) Directors as they are the strategic planners for NIST operations. NIST OUs must be aware of the Department of Commerce (DOC) real property policies, NIST's implementation of those policies, and the timeline to accomplish the processes.

REFERENCES

- [15 U.S.C. § 278c - Acquisition of Land for Field Sites](#)
- [42 U.S.C. § 55 - National Environmental Policy Act \(NEPA\)](#)
- [Department of Commerce Real Property Management Manual, August 2014 and subsequent revision \(RPMM\)](#)
- [P 2100.00 Site and Facilities Management Policy](#), (8/28/2015)

DEFINITIONS

Acquisition – The process of gaining ownership or control of real property or interest in real property.

Disposal – The process of relinquishing ownership or control of real property or interest in real property.

Real Property Action – For the purposes of this directive, refers either to an acquisition or a disposal.

Real Property Contracting Officers (RPCO) – warranted contracting officers who are specifically trained for the purpose of administering federal real property acquisitions.

REQUIREMENTS

The [DOC Real Property Management Manual \(RPMM\)](#) requires NIST to meet specific requirements which include.

- Initiate requests for real property actions, by contacting an appropriate office that is responsible for real property issues, and coordinate such requests with the DOC Office of Real Property Programs (ORPP);
- Assist with the development of required asset acquisition documentation;
- Coordinate with the Department of Commerce Office of Facilities and Environmental Quality (OFEQ) and other Departmental counterparts when approval or guidance relating to policy issues concerning real property acquisition, management, utilization, and disposal are required;
- Coordinate and provide ORPP with advance notice of all requests for, and acceptance of, General Services Administration (GSA) real property delegations of authority, except for the delegations specified in the RPMM and Contracting Officer Representative (COR) delegations;
- Acquire real property and interests in real property in a manner that is consistent with site-specific workspace plans and DOC portfolio management plans, and, as applicable, local portfolio plans and goals;
- Provide ORPP with advance notice of all real property disposal, transfer, and exchange actions;
- Periodically assess real property assets that are either less than fully utilized or underutilized to determine if co-location, consolidation, or disposal is appropriate;
- Recommend real property assets to ORPP for disposal;
- Coordinate the screening, reassignment, transfer, or disposals of unneeded assets, and provide funding and management of the asset while it is under control of the OU; and
- Verify and maintain the accuracy of NIST information entered into the Federal Real Property Management (FRPM) database.

AUTHORITIES

The NIST Director has delegated the authority and responsibility to the Chief Facilities Management Officer for NIST's compliance with the requirements set forth in this document.

ROLES AND RESPONSIBILITIES

The NIST Director shall:

- Determine when NIST shall seek to acquire or divest real property assets.

The Chief Facilities Management Officer (CFMO) shall:

- Make recommendations to the NIST Director as to the proposed real property action.
- Follow the processes defined by the RPMM to implement the NIST Director's decision on proposed real property acquisition and/or disposal actions.

OU Directors shall:

- Seek space solutions within NIST owned spaces as defined within the Space Management Order and Procedure prior to seeking acquisition of additional facilities.
- Notify the CFMO when real property assets are no longer being fully utilized.

The Office of Acquisition and Agreements Management shall:

- Assist the CFMO by providing the support of a Real Property Contracting Officer to execute and administer the real property acquisitions.

The Office of Safety, Health and Environment shall:

- Assist the CFMO in compliance with the NEPA documentation for the real property action.

The Office of Financial Resource Management's Budget Division shall:

- Seek Congressional approval for acquisition of real property assets through the process defined in the RPMM.
- Ensure that funds for the purchase of real property and its related administrative and legal costs are authorized, which shall include, but may not be limited to, appraisal fees, the real property purchase price, and advertising fees.

PROCEDURES

NIST staff shall follow the procedures in the [RPMM](#), including:

- Chapter 8 – Acquisition of Real Property
- Chapter 11 – Disposal of Real Property

DIRECTIVE OWNER

190 – Office of Facilities and Property Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	1/20/2016	John Bollinger	Initial Draft
Rev. 1	1/20/2016	Dan Cipra	Formatting Updates
Rev. 2	1/24/2016	John Bollinger	Addressed comments from Dan Cipra
Rev. 3	2/25/2016	John Bollinger	Inserted updates provided by OAAM
Rev. 4	3/18/2016	John Bollinger	Addressed comments from DRB members

Leasing of Real Property

NIST S 2103.06

Issue Date: 3/23/2016

Effective Date: 3/23/2016

PURPOSE

To provide guidance on the responsibilities and procedures for the leasing of real property assets (i.e., Class 1 land and/or Class 2 buildings/structures) in support of the National Institute of Standards and Technology (NIST) mission.

APPLICABILITY

In addition to the Office of Facilities and Property Management, this order applies to all NIST Organizational Unit (OU) Directors as they are the strategic planners for NIST operations. NIST OUs must be aware of the Department of Commerce (DOC) real property policies, NIST's implementation of those policies, and the timeline to accomplish the processes.

REFERENCES

- [15 U.S.C. § 278e – National Institute of Standards and Technology – Functions and Activities](#)
- 42 U.S.C. § 55 – [National Environmental Policy Act \(NEPA\)](#)
- [Department of Commerce Real Property Management Manual, August 2014 and subsequent revision \(RPMM\)](#)
- [P 2100.00 Site and Facilities Management Policy](#), (8/28/2015)

DEFINITIONS

Real Property Action – For the purposes of this directive, refers to initiating or terminating a lease agreement.

Real Property Contracting Officers (RPCO) – Warranted Contracting officers who are specifically trained for the purpose of administering federal real property acquisitions.

REQUIREMENTS

The DOC Real Property Management Manual (RPMM) requires NIST to meet specific requirements such as:

- Initiate requests for real property actions by contacting an appropriate office that is responsible for real property issues, and coordinating such requests with the DOC Office of Real Property Programs (ORPP).
- Monitor and enforce the terms and conditions of leases.

- Implement General Services Administration (GSA) delegations of authority for the operation and maintenance of Federally-owned buildings and administration of GSA leases.
- Nominate on-site representatives to serve as Contracting Officer's Representatives (CORs) for DOC and GSA-delegated leases, as appropriate.
- Serve as the Contracting Officer's Representative (COR), as requested, for alterations and repairs, and monitor quality control and conformance with specifications.
- Serve as liaison, except where the COR has been designated, with GSA Regional Offices on daily operational matters.
- Verify square footage and classification assignments for the GSA rent bills.
- Assist ORPP with the verification of rent and reconciliation of discrepancies with GSA.
- Perform condition survey reports, at the request of GSA or DOC Office of Facilities and Environmental Quality (OFEQ), to document the condition of DOC leased space at time of occupancy and upon vacating the space.

AUTHORITIES

In the performance and function of the Institute, the Secretary of Commerce is authorized to undertake the rental of field sites and laboratory, office, and warehouse space. ([15 U.S.C. 278e](#)).

ROLES AND RESPONSIBILITIES

The NIST Director shall:

- Determine when NIST shall seek to acquire leased space or terminate a lease agreement.

The Chief Facilities Management Officer (CFMO) shall:

- Make recommendations to the NIST Director as to the proposed real property leasing action.
- Follow the processes defined by the RPMM to implement the NIST Director's decision on proposed real property leasing actions.

OU Directors shall:

- Seek space solutions within NIST owned spaces as defined within the Space Management Order and Procedure prior to seeking acquisition of additional facilities.
- Provide funding for the leasing process and the annual costs associated with the lease agreement.
- Notify the CFMO when leased space is no longer being fully utilized.

The Office of Acquisition and Agreements Management shall:

- Assist the CFMO by providing the support of a Real Property Contracting Officer to execute and administer the real property acquisitions.

The Office of Safety, Health and Environment shall:

- Assist the CFMO in compliance with the National Environmental Policy Act (NEPA) documentation for the real property action.

The Office of Financial Resource Management's Budget Division shall:

- Ensure that OU funds for the annual lease costs and its related administrative and legal costs are authorized.

PROCEDURES

After confirming that a real property lease is the more economical and practical solution to address a valid NIST space requirement, NIST shall contact the DOC ORPP to engage with the GSA and utilize their services to meet the validated requirement. Since the needed space is not available on the NIST campuses, GSA may pursue space for NIST in other federal space or in leased space, as GSA and NIST jointly deem appropriate. NIST shall work with ORPP and the legal offices of NIST and the Department's Real Property and Environmental Law Division in the Office of the General Counsel, and shall abide by the guidance contained in the DOC RPMM.

NIST staff shall follow the procedures in the RPMM, including:

- Chapter 6 – General Services Administration Transactions, Delegations, and Prospectus Level Projects
- Chapter 8 – Acquisition of Real Property

PROHIBITED ACTIONS OF NIST EMPLOYEES AND AFFILIATES

Unless authorized in writing by the RPCO, officials and employees of NIST must at no time, either directly or indirectly, contact lessors, offerors or potential offerors for the purpose of making oral or written representations, commitments, or agreements with respect to agency needs or preferences, lease terms, occupancy of particular space, tenant improvements, alterations and repairs, or overtime services. This prohibition includes the period before and after a request for space is submitted to the RPCO, and after a lease is executed.

DIRECTIVE OWNER

190 – Office of Facilities and Property Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	1/20/2016	John Bollinger	Initial Draft
Rev. 1	1/20/2016	Dan Cipra	Formatting Updates
Rev. 2	1/24/2016	John Bollinger	Addressed comments from Dan Cipra
Rev. 3	2/25/2016	John Bollinger	Added comments from OAAM
Rev. 4	3/18/2016	John Bollinger	Addressed comments from DRB members

Mail Management

NIST PR 2103.05
Effective Date: 8/10/2016

PURPOSE

The purpose of this Directive is to establish the responsibilities and procedures for the handling of official mail at the National Institute of Standards and Technology (NIST). It is the goal of this program to process and deliver all mail in a proficient, professional, and timely manner. This directive replaces Administrative Manual Subchapter 4.07 Mail Management.

APPLICABILITY

This document applies to NIST Boulder and Gaithersburg locations. Mail procedures for other locations are controlled by the management of those sites.

REFERENCES

- [41 CFR Part 101-9 \[FPMR Amendment A-53\] Entitled “Federal Mail Management”](#)
- [18 U.S. Code Chapter 31, Paragraph 1719, entitled “Franking Privilege”](#)
- [39 U.S. Code Chapter 32 – “Penalty and Franked Mail”](#),
- [U.S. Postal Service \(USPS\), "Domestic Mail Manual, “](#)
- Department of Commerce “Mail Management Manual” (under revision),
- [Package Services – Gaithersburg \(inet service page\)](#)
- [Mailroom Services – Boulder \(NOAA provided\) \(inet service page\)](#)

DEFINITIONS

Franked Mail - Mail with an official mark enabling it to be sent free of charge.

Penalty Mail - Mail with an official mark on (a piece of mail) so that it can be sent free of charge with a “Penalty for Private Use” statement.

RESPONSIBILITIES

Office of the Director

- Direct the Chief Facilities Management Officer (CFMO) to establish a NIST-wide Mail Management Program in accordance with [41 CFR Part 101-9, \(FPMR Amendment A-53\)](#)

Chief Facilities Services Division (FSD)

- Designate a NIST Mail Management Program Manager to be responsible for establishing an effective and efficient NIST Mail Management Program.
- Appoint an individual responsible for the management of the NIST Mail Management Program in accordance with 41 CFR Part 101-9, (FPMR Amendment A-53) entitled “Federal Mail Management”.

Director of International and Academic Affairs Office (IAAO)

- Clear all foreign mail and packages.

NIST Mail Management Program Manager

- Effectively and efficiently manage day-to-day operations of the NIST Mail Management Program in accordance with all applicable Federal Laws, regulations and policies.

NIST Facilities Services Division (FSD) Package Services Group

- Order specially printed envelopes, brochures, mailing labels, self-mailers, and other required supplies.

Mailroom Staff

In Boulder	In Gaithersburg
NOAA Facilities and Operations Division (FOD) Mail Room Staff	OFPM FSD Package Services Group

- Process incoming and outgoing mail (USPS, interagency, and intra-NIST mail). This includes any mailing services accomplished by outside contractors;
- Determine the postage paid by NIST to the United States Postal Service and keep an accurate record of all postage usage. Negotiate with the Postal Service when any discrepancies occur.

Division Chief or equivalent

- Designate mail delivery and pickup points;
- Ensure that NIST mail addresses of employees, guest researchers, and research associates and Divisional mailing and distribution lists are kept up to date.

NIST Forms Management Officer

- Prepare requests for the signature of the NIST Director to the Department of Commerce for permission to obtain special mailing envelopes.

NIST Employees

- Ensure that mail sent to NIST addresses is for official business (personal mail is to be sent to personal addresses only);
- Use envelopes with the NIST return address solely for official NIST business.
- Obtain written approval from the NIST Mail Management Program prior to entering into any purchase order/contract or other method of obligating NIST for the payment of postage.
- Follow all government regulations with regard to mailing practices.
- Forward to the NIST Office of the Director all mail received from the Congress.

PROCEDURES

Mail Stops

- Mail stops are designated mail delivery and pickup points requested by a memorandum (See Appendix A for sample memo) approved by the Division Chief or equivalent, to the supervisor of the FSD Package Services Group. Requests for the establishment of mail stops are subject to the final approval of the NIST Mail Management Program Manager. The number of mail stops shall be kept to a minimum.
- Mail stops are required for internal mail. The formats for addressing internal mail are:
 - In Gaithersburg: [recipient name] – STOP [xxxx] (stop must equal four digits)
 - In Boulder: [recipient name] – MC [xxx.xx] (stop must equal three digits, decimal point, and two more digits)

Official Return Address

- To avoid delay or possible return of mail, all official mail must include the official return address (shown below) in the upper left corner of the envelope (or address label if official postage is to be affixed.) In addition, the appropriate four-digit mail stop must be included under the return address.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899-[xxxx]
OFFICIAL BUSINESS PENALTY FOR PRIVATE USE, \$300
Return Service Requested 20899-[xxxx]

MS [xxxx]

(In place of the sender's individual operating unit mail stop and zip code plus-four digits, the following may be used: "Public and Business Affairs Division 20899-3460".)

- Changes to employee's official NIST mailing address are made through the Directory Request section of the [NIST 1221 Form](#) (Only administrative and/or support staff can complete and submit this form for the employee.)

Mail Delivery Service

- In Gaithersburg: Mail is delivered to and collected at NIST mail stops once each day, Monday - Friday. Under normal conditions, the mail collected on any pickup is delivered anywhere at NIST-Gaithersburg on the next scheduled delivery. The schedule is:

TRUCK I – 8:30-11:00 a.m. Buildings 220, 222, 225, 235

TRUCK I – 1:30-3:30 p.m. Buildings 101, 103, 207, 227, 230, 231, 233, 318, 320

TRUCK II- 8:30-11:00 a.m. Buildings 221, 223, 224, 226

TRUCK II- 1:30-3:30 p.m. Buildings 202, 203, 205, 215, 216, 217, 218, 219, 303, 304, 411

(Under certain circumstances, special messengers may be available in Gaithersburg upon request. Contact the Package Services Staff at extension 8393, 5511 and 6051 for more information.)

- In Boulder: Mail is delivered to and collected at mail stops once per day by 10:00 a.m.

Incoming Mail

- In Gaithersburg: Incoming mail is delivered by the United States Postal Service (USPS) to the NIST Package Services Group at 8:30 a.m. There is no direct USPS Delivery service to individual recipients. Mail from Main Commerce is picked up and delivered to NIST by courier service through the Package Services Group.

Mail (both USPS and intra-NIST) is delivered to the mail stop of the addressee unopened with the following exceptions:

- Mail from the White House, the Congress, and the Secretary of Commerce is delivered unopened to the Office of the Director, NIST.
 - Mail addressed to "The Director" is delivered unopened to the Office of the Director, NIST.
 - Mail addressed to the "National Institute of Standards and Technology" is opened and routed by Package Services Group Leader.
- In Boulder: Incoming mail is delivered by the USPS to the NOAA Facilities and Operations Division Mail Room at 7:00 a.m. and picked up at 10:00 a.m. and 2:30 p.m.
- Mail (both USPS and intra-NIST) is normally delivered unopened to the addressee (Mail with an insufficient address is opened and routed). The additional processes exist:

- Books and periodicals are delivered to the Library.

- Employees should report all mail from Congress to the Office of the Director, NIST/Boulder Laboratories which contacts the Office of the Director, NIST.
- Certified and Registered Mail – Signature of the addressee is required for delivery. If the addressee receives mail accompanied by Return Receipt ([USPS Form 3811, Domestic Return Receipt](#)), the addressee signs the receipt when the mail is received and gives the signed receipt to the messenger.
- Packages not addressed to a specific person and/or packages with a NIST purchase order number are opened by Package Service Group Leader and re-routed to the proper organizational unit.

Redirection of Incoming Mail

On occasion, mail may be inadvertently delivered to the wrong mail stop. When this occurs, immediately redirect the mail to the proper mail stop, if known, or return it to Package Services for routing with notation "misaddressed."

Unwanted Incoming Mail

Advertisements, books, letters, magazines, and material from mass mailing lists are often sent to staff members at NIST. If the addressee does not want this material, write "REFUSED" beside the crossed-out address and place the material in the outgoing mail tray. The mail is returned to the sender by the USPS. If the addressee has left NIST or has died, "NO LONGER AT NIST" or "DECEASED" should be written on the material in place of "REFUSED."

Mail in the following classes addressed to a former employee and not connected with officially assigned work may be forwarded:

- (1) First-class mail (including zone-rated Priority Mail) and post and postal cards;
- (2) Express mail;
- (3) Official mail that is sent as first-class mail;
- (4) Second-class mail;
- (5) Third-class mail when the sender has guaranteed to pay the forwarding postage; and
- (6) Fourth-class mail locally or when the sender has guaranteed to pay forwarding postage.

NOTE: The address (but not the name) may be changed and the mail forwarded as many times as necessary to reach the addressee.

The proper way to forward mail is to place a line through the address (but do not obliterate or cover it up). Near the address write "Forward To" and the new address where the mail should be forwarded. Do not cover the original address with a label and do not put mail in an envelope with the NIST return address. Former NIST employees should be asked to notify their correspondents of their new address.

Outgoing Mail

In Gaithersburg:

- Outgoing USPS Mail is picked up from the Package Service Group at 4:00 p.m. each workday.
- Gaithersburg mail to Main Commerce is picked up from the Package Services Group, Director's Office, Travel Office and Accounts Payable by the NIST courier daily and delivered to the Commerce Mail Room and assigned mail delivery locations at 8:30 a.m., 12 p.m., and 2:30 p.m.
- Urgent mail from NIST Gaithersburg to NIST Boulder is picked up from Package Services at 4:00 p.m. each workday. For best service, the mail codes for Boulder organizational units should be prominently displayed on envelope return addresses and letterheads.

In Boulder:

- Outgoing mail is dispatched from the NOAA Facilities and Operations Division Mail Room to the Boulder Post Office at 2:30 p.m.
- Urgent mail from NIST Boulder to NIST Gaithersburg is most expeditiously handled by attaching a blue dot for identification. The Package Service Group puts all mail with a blue dot in an overnight pouch and takes it to the Post Office daily at 2:30 p.m.

Packages

- Package Services staff do not have packaging facilities.
 - In Gaithersburg: If the sender cannot wrap and seal material, prepare [NIST Form-386, Shipping Order](#), and notify Shipping and Receiving to arrange for pick up, packaging, and delivery of material to Mail and Distribution for dispatch. Shipping and Receiving also handles all shipments by commercial carrier except the GSA contract carrier.
 - In Boulder: NOAA FOD Shipping and Receiving staff provide similar services as those in Gaithersburg. The staff does wrapping, sealing, and shipping of domestic or foreign packages. The sender should prepare [Form BL-50, Shipping Document](#).
- Mail and packages to foreign countries, after clearance by the Director of International and Academic Affairs Office (IAAO) if required, must be referred to the campus's Package Services Group for the necessary customs label and declaration. [Click here](#) for a list of those countries requiring clearance by the Director of IAAO. Packages not bearing required information may be delayed, opened, and returned to NIST.

DIRECTIVE OWNER

190 – Chief Facilities Management Officer

APPENDICES

- A. Mail Stop Request Memorandum Sample
- B. Revision History

APPENDIX A

MAIL STOP REQUEST MEMORANDUM SAMPLE

NIST MAIL CENTER
MAIL STOP CHANGE REQUEST

(Please provide two weeks' advance notice)

(Submit to Stop 1921/ Building 301 Rm B185 or email michelle.wims@nist)

DATE: _____ REQUESTING DIVISION/OFFICE/GROUP: _____

CONTACT: _____ TELEPHONE: _____

Indicate type of change(s):

Mail Stop Information:

___Provide New Mail Stop

Customer Provide New Location _____
New _____ (will be assigned by Michelle Wims)

___Remove Current Mail Stop

Current Stop & Location _____

___Move Current Mail Stop Location

Current Stop & New Location _____

Secretary assigned to new mailstop: _____

DATE CHANGE REQUIRED: _____

AUTHORIZING OFFICIAL: _____

(Signature and Date)

MAIL STOP # WILL SERVE THE FOLLOWING EMPLOYEES:

EMPLOYEE

EMPLOYEE

(If necessary, use additional sheets)

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	2/8/2016	Virginia Holtzman-Bell	Initial Draft
Rev. .01	2/12/2016	Dan Cipra	Formatting updates only
Rev. .02	8/2/2016	Michelle Wims	Updated with DRB Comments

Site Access During Site Closure and Delayed Openings

NIST O 2105.00
Effective Date: 2/10/2015

PURPOSE

This directive establishes the NIST requirements and responsibilities for restricting access to NIST sites during Site Closure or Delayed Opening situations. The declaration of Site Closure or Delayed Opening is part of the NIST risk management of personnel and facilities. This Order will replace Administrative Manual Subchapter 6.02, Emergency NIST Arrival, Dismissal and Closure.

APPLICABILITY

This directive applies to all NIST owned or administered sites and affects NIST, and all other federal agency employees, associates and visitors located at those sites.

REFERENCES

- [NIST Emergency Management Policy, P 410.01](#);
- [Office of Personnel Management's Washington, DC, Area Dismissal and Closure Procedures](#);
- [Telework Enhancement Act of 2010 \(Public Law 111-292\)](#); and
- [Telework Program Directive, NIST Order 3102.00](#).

DEFINITIONS

Emergency Employees – Individuals designated in writing who, by nature of their work, are deemed critical to agency operations (including safety, security and operations and maintenance) and are therefore required to remain on duty or report for duty during emergencies when other employees are generally dismissed.

Site – NIST owned or administered physical locations.

Site occupants – Federal employees, associates of federal agencies, NIST associates, guest researchers, contractors, vendors, suppliers, or visitors physically located at the site.

REQUIREMENTS

- Provide guidance for the safety and security at NIST-administered sites.
- Establish the responsibilities and authorities for site closure and delayed openings.

- Establish procedures for the determination of site operating status and for notification and dissemination of that status.

Based on the above requirements, management has established a series of site status decisions.

Site Status Decisions:

Site is closed (with access only for emergency employees).

- Designated emergency employees must report to work as scheduled.
- No access will be granted to non-emergency personnel without approval by their management chain.
- The site is closed for onsite business and no public access is permitted.
- Telework-ready employees must follow DOC/NIST guidance and the terms of their agreements.
- Site closure vehicle access procedures will be put in place.

Site is closed with limited access.

- Designated emergency employees must report to work as scheduled.
- The site is closed for onsite business and no public access is permitted.
- Telework-ready employees must follow DOC/NIST guidance and the terms of their agreements.
- Non-emergency employees / associates (facility users) who are currently authorized 24x7 access and who have a legitimate requirement to access the site, can be granted access, subject to site conditions.
- Site closure vehicle access procedures will be put in place.

Delayed opening at “a designated time,” unscheduled leave or unscheduled telework authorized.

- Designated emergency employees must report to work as scheduled.
- The site is closed for business and no public access will be permitted prior to the announced time of the delayed opening.
- Access will be on the same basis as when NIST is closed with limited access.
- Non-emergency employees / associates (facility users) who are currently authorized 24x7 access and who have a legitimate requirement to access the site, can be granted access, subject to site conditions.
- Telework-ready employees must follow DOC/NIST guidance and the terms of their telework agreements.
- Non-emergency employees / associates must notify their supervisor of their intent to use unscheduled leave or unscheduled telework.

Site is open with the option of unscheduled leave or telework.

- Designated emergency employees must report to work as scheduled.

- The site is open for business, but special flexibility is offered for those who cannot commute safely to work.
- Telework-ready employees must follow DOC/NIST guidance and the terms of their telework agreements.
- Non-emergency employees / associates must notify their supervisor of their intent to use unscheduled leave or unscheduled telework.

Site will close at “a designated time” for onsite business due to early dismissal

- Designated emergency employees must remain at work as scheduled.
- The site is closed at a designated time for onsite business and no public access is permitted.
- Telework-ready employees must follow DOC/NIST guidance and the terms of their agreements.
- Non-emergency employees / associates (facility users) who are currently authorized 24x7 access and who have a legitimate requirement to access the site, can be granted access or remain on site, subject to site conditions.
- Site closure vehicle access procedures will be put in place.

RESPONSIBILITIES AND AUTHORITIES

Associate Director for Management Resource (ADMR):

- Publishes annual notice or memorandum letter designating NIST emergency employees who will be allowed access during site closure.
- Is the Site Designated Official for Gaithersburg, MD.
- Assigns the Boulder Laboratory Site Manager as the Site Designated Official for Boulder, CO.
- Aligns NIST procedures with Office of Personnel Management (OPM) published guidance, as appropriate. NIST’s intent is to build upon the OPM procedures protecting our staff while continuing the Government’s vital business.

Organizational Unit (OU) Directors

- Provide names and/or positions of staff to be designated as emergency employees to the Site Emergency Coordinator.
- Grant exceptions for access under site specific procedures, when necessary and as appropriate.
- Develop OU specific procedures for the implementation of this Order.
- Ensure employee compliance with this Order.

Chief Facilities Management Officer (CFMO)

- Establishes and publishes procedures implementing this Order on NIST sites.
- Implements procedures described above during an event.

- Prepares the annual list of emergency employees for the Associate Director for Management Resources to promulgate the annual designation letter.
- Establishes notification systems to alert site occupants and the general public as to site status.

Site Emergency Coordinator

- Implements site status changes and notifications for the applicable site.
- Creates and maintains emergency employees' lists.
- Enforces procedures during site closure or delayed opening at NIST sites through the Police Services Group.
- Position within the Emergency Services Division

Supervisors

- Identify potential emergency employees to OU Director for inclusion in annual designation letter.
- Communicate requirements of this directive to both emergency and non-emergency employees.
- Implement OU specific procedures.

Emergency employees

- Report or remain on duty to support and sustain agency operations even during protracted events.
- Be familiar with and prepared to perform actions as designated in the memorandum letter – *“Emergency Employee” Positions at the National Institute of Standards and Technology*.

Site Occupants (as applicable)

- Be familiar with and comply with the procedures implementing this directive.
- Use and respond to the site status notification systems.
- Follow their federal agency/company employer procedures during these events with regard to work status.
- Exercise personal responsibility for their safety and use good judgment in planning their commute.
- Notify their supervisors in a timely manner of their intentions to use unscheduled leave or unscheduled telework.

Teleworkers

- Have an established telework agreement that includes expectations for working from off-site during situations of site closure or delayed opening.

DIRECTIVE OWNER

130 – Associate Director for Management Resources

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	7/3/2013	Mark Spurrier	Initial Draft
Rev .01	7/9/2013	Dan Cipra	Formatting Changes
Rev .02	1/28/2015	Dan Cipra	Implemented DRB corrections

Transportation Program

NIST O 2106.00
Effective Date: 2/23/2016

PURPOSE

This directive establishes authorities, requirements, and assignment of responsibilities for the National Institute of Standards and Technology (NIST) Transportation Program. Elements of the program include the use and management of government-owned or -leased motor vehicles, shuttle services, and the transit subsidy. This order replaces Administrative Manual Subchapters 2.07, 2.08 and 2.10. Not all programs are available in all NIST locations. Procedures promulgated subsequent to this order will provide the extent of the program availability.

APPLICABILITY

This directive is applicable to all Federal employees and contractors to the extent allowed by law and the terms of the contractor's agreement.

REFERENCE

- [Federal Management Regulation FMR102-34](#)
- [United States Code 40 USC 17503](#)
- [United States Code 31 USC 1344](#)
- [United States Code 31 USC 1349](#)
- [Code of Federal Regulations 5 CFR 930.105, 111, and 112](#)
- [Code of Federal Regulations 49 CFR Part 383](#)
- [GSA Bulletin FMR B-30 Motor Vehicle Management](#)
- [Executive Order 13150 - Federal Workforce Transportation](#)
- [OMB Memorandum M-07-15 - Federal Transit Benefits Program](#)
- [P 2100.00 Facilities and Site Management Policy](#) (8/28/2015)

DEFINITIONS

- Commercial Driver's License (CDL) – A license issued to an individual by a State or other jurisdiction of domicile, which authorizes the individual to operate a class of a commercial motor vehicle.

- Government Motor Vehicles – Vehicles (Department of Commerce owned and GSA leased) that are operated in performance of their duties. Some examples of vehicle types include sedans, light/medium/heavy duty trucks, cargo/passenger vans, buses, and emergency vehicles.
- Motor Vehicle Operator (MVO) – All personnel that operate a government-owned or -leased motor vehicle.
- Shuttle Services – Standard bus or van passenger services to and from events, Metro Rail and MARC commuter connection points.
- Transit Subsidy Program – A government program that defrays the cost of commuting to and from work to individuals using an approved transit solution.
- Vehicle Allocation Methodology (VAM) – A standard means of ensuring that each vehicle in the fleet is correctly sized and appropriate for accomplishing the NIST mission as specified in General Services Administration (GSA) Bulletin FMR B-30 Vehicle Allocation Methodology (VAM) for Agency Fleets.

REQUIREMENTS

Government Vehicles

- NIST shall establish a government vehicle program to ensure compliance with applicable references. Program shall include GSA leased vehicles and government-owned vehicles at all NIST locations.
- Requests for the short-term (less than 3 years) and long-term (3 years or greater) assignment of government vehicles shall be made in accordance with Transportation Services Group standard operating procedures.
- MVO's shall abide by all applicable laws, policies, and regulations.
- The Fleet Manager shall make long-term assignment of government vehicles to Organizational Units (OU) in accordance with the OU's mission needs, and VAM. Long-term is typically until the vehicle is no longer needed. Requests for reassignment of vehicles shall be made to and approved by the Fleet Manager.
- Requests for modifications or special equipment to be installed on government vehicles shall be approved by the Fleet Manager. All modifications need to be removed and all damages repaired prior to return of the vehicle. The OU shall arrange for any damage repairs through the Fleet Manager. The OU assigned the vehicle is financially responsible for these costs.
- The Fleet Manager shall re-evaluate assignment of Government vehicles to OUs, on a semi-annual basis, at a minimum, for need and cost effectiveness.
- Government vehicles shall be acquired, maintained, and replaced in accordance with Transportation Services Group and GSA policies and procedures, as applicable.
- Federal employees who are required to hold a CDL shall ensure they remain in good standing in their State-of-Record, maintain up-to-date medical certification, and hold any required endorsements.

- Government vehicles may not be used to transport hazardous, as defined under 40 CFR 261, or universal waste, as defined under 40 CFR 273, onto the NIST Boulder or WWV/WWVB facilities. State regulations may contain additional requirements.
- Use of government vehicles is restricted to official purposes. Federal employees or contractors assigned to government vehicles shall take annual training on official use of government vehicles. This training is offered on Commerce Learning Center (CLC). Use of government vehicles in the transportation of employees between their homes and places of employment is prohibited.

Shuttle Services

- Shuttle services shall be provided in support of NIST mission requirements and the Transit Subsidy Program.
- Only NIST federal employees, NIST associates, and visitors on official business shall be permitted to ride the shuttle.

Transit Subsidy

- Establish a transit subsidy program to ensure compliance with applicable references.
- NIST federal employees who meet the criteria for transit subsidies shall be eligible to participate in the Transit Subsidy Program.
- Subsidy participants shall inform the Local Transit Subsidy Program Coordinator of any changes in eligibility including withdrawing from the program.

RESPONSIBILITIES AND AUTHORITIES

NIST Director

- Authorizes the establishment of a Transit Subsidy program and delegates the responsibility for the program to the Chief Facilities Management Officer (CFMO).
- Authorizes the CFMO to manage the government vehicles program for NIST.
- Authorizes the shuttle service program for NIST Gaithersburg and delegates its management to the CFMO.

Chief Facilities Management Officer

- Manages the Transportation Management Program.
- Delegates management of the program to the Facilities Services Division and the Transportation Services Group.

OU Directors

- Determine mission need for long-term assignment of government vehicles.
- Responsible for the costs incurred by NIST for OU-assigned vehicles and their staff for transit subsidy benefits.

- Manage the program within their OU for proper operation of government vehicles, and staff participation in the transit subsidy program.

Transportation Services Group Supervisor

- Develops and maintains an effective transportation program in accordance with GSA regulations and Department of Commerce guidance.

Local Transit Subsidy Program Coordinator

- Manages the Transit Subsidy Program.
- Manages the daily requirements for enrolling and removing employees from the Transit Subsidy Program.
- Creates accounts for employees to use SmarTrip card for receiving the transit subsidy benefit.
- Bills appropriate Division or Group for transit subsidy benefits used.

Fleet Manager

- Manages the day-to-day operation of the fleet, to include ordering tags, fleet cards, vehicle replacements and vehicle maintenance.
- Provides required correspondence to GSA and the Department of Commerce.
- Responsible for maintaining accurate inventory of all vehicles for NIST in MD, CO and HI and ensures all vehicles adhere to the VAM.
- Responsible for maintaining serviceable fuel tanks and ensuring availability of all fuel types.
- On a bi-annual basis, ensures that employees with CDLs are in good standing in the states where they hold a civilian license.
- Ensures that medical certificates are up-to-date for all drivers required to carry them.
- Considers all requests for modifications or special equipment to be installed on government vehicles.
- Manages shuttle and bus services, and short-term vehicle rental needs in support of mission requirements.
- Bills appropriate division or group for use/maintenance of government vehicles, ensures lease payments are made to GSA, verifies fleet card charges, and ensures payment is made to the fleet card vendor.

Motor Vehicle Operators (MVO)

- Safely operates government vehicles and adheres to all motor vehicle laws and regulations.
- Performs user maintenance checks of vehicles prior to use.
- Reports any maintenance concerns.

- Reports accidents to the Fleet Manager.
- Maintains a valid state driver's license in good standing with their state of issuance before operating a government vehicle.
- If required to hold a CDL, maintains up-to-date medical certification and holds any required endorsements.

Transit Subsidy Participants

- Files necessary subsidy requests to their program manager in accordance with NIST Transit Subsidy procedures.
- Immediately reports any changes that would impact eligibility or subsidy amount to the Local Transit Subsidy Coordinator.

DIRECTIVE OWNER

190 - Office of Chief Facilities and Property Management Officer

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	29 Mar 13	David Henry (Chief, FSD)	First Draft
Rev. 1	8 Apr 13	Vivian Shirley (FSD)	Incorporated comments from Transportation Services Group
Rev. 2	17 Apr 13	Vivian Shirley (FSD)	Incorporated comments from Emergency Services Division
Rev. 3	29 Apr 13	Vivian Shirley (FSD)	Final Draft with Chief, FSD edits
Rev. 4	30 Apr 13	Vivian Shirley (FSD)	Final Draft, incorporating comments from EMSS Boulder

Traffic and Parking

NIST PR 2106.01

Effective Date: 01/17/2014

PURPOSE

This directive contains traffic and parking procedures applicable to the grounds of the National Institute of Standards and Technology (NIST) at Gaithersburg, Maryland and Boulder, Colorado, including responsibilities and program details.

APPLICABILITY

The directive is applicable to all Employees, Associates and Visitors at the Gaithersburg, Maryland and Boulder, Colorado sites.

REFERENCES

- [15 C.F.R. Part 265](#)—Regulations Governing Traffic and Conduct on the Grounds of the National Institute of Standards & Technology, Gaithersburg, Maryland and Boulder and Fort Collins, Colorado, as amended (NIST Traffic and Parking Regulations).
- [15 U.S.C. 278e\(b\)](#) – NIST Functions and Activities
- [42 U.S.C. 12101](#), et seq., Americans with Disabilities Act of 1990, as amended

DEFINITIONS

Carpools – For purposes of this directive, a carpool is a group of two or more individuals who work at NIST and share use of a motor vehicle for transportation to and from work. The term carpool also includes vanpools.

NIST Facility Access Card (FAC) – name provided for a visually identifiable card that represents the various card types issued by the NIST Badge Office.

Properly Permitted Motor Vehicles – Vehicles with current state licensing, current motor vehicle insurance and a NIST-issued parking permit.

RESPONSIBILITIES

Chief Facilities Management Officer (CFMO)

- Establishes and posts speed limits and determines the location of traffic control signs and roadway markings on the NIST site.
- Except as otherwise authorized herein, designates areas for reserved and temporary parking spaces.

Chief of Emergency Services Office

- Functions as the manager for the parking program.
- Approves all requests for new or modifications to existing parking spaces.

Department Of Commerce Office of Security Police Services Group (DOC OSY PSG)

- Closes roads and/or facilitates the towing of vehicles for traffic or other emergencies (Such as: blocking emergency response vehicle access, loading docks, and impeding maintenance projects, as well as to address abandoned vehicles).
- Enforces NIST Traffic and Parking Regulations on the site including Maryland and Colorado law as applicable.
- Issues warnings and citations for violations of NIST Traffic and Parking Regulations.

NIST Employees

- Obtain a valid parking permit for all non-government vehicles to be operated on site.
- Properly display the parking permit so that it is clearly visible.
- Operate only properly registered motor vehicles on the site.
- NIST employees who sponsor visitors must inform them of these parking restrictions.
- Comply with 15 C.F.R. Part 265 and all NIST traffic and parking procedures.
- Drive in a safe manner on the NIST campuses.

PARKING

Parking Permit Display and Use

- A parking permit is an authorization to use any available, unrestricted parking space, but it does not guarantee a space will be available in the location desired.
- Parking Permits are non-transferrable and are only valid for the individual to whom they were issued.
- Permits must be properly displayed; failure to display properly can result in a citation.
- Parking permit rearview mirror hanger tags must be displayed on the reverse side of the vehicle's rear view mirror.
- Permits are not required for motorcycles or motor scooters.

Parking Limitations

- Vehicles shall be parked in designated parking spaces only.
- Only authorized vehicles shall be parked in reserved special category parking spaces as defined below.
- Parking along roadways, fire lanes, interior paths, on grass plots or in landscaped areas is strictly prohibited (authorized construction and maintenance vehicles are exempted from this prohibition).
- Vehicles authorized to park in reserved special category spaces may also park in any available, unrestricted space.
- Enforcement of carpool parking spaces is in effect from 7:30 a.m. to 10:30 a.m. Monday through Friday, excluding federal holidays.

- During special events, parking is permitted in any space only when directed by DOC OSY PSG uniformed personnel.

PROCEDURES

Parking Permit Registration

- NIST employees/associates with a valid NIST FAC who desire a parking permit must complete the [Form NIST-201, Parking Permit Registration](#), and submit in person to the Badge Office. A parking permit should be requested for each personal vehicle that will be used on the site.
- All visitor vehicles entering NIST sites will be issued a temporary parking permit. The visitor temporary parking permit includes an expiration date based on the duration of the visit.

Reserved Parking for Special Categories

Reserved parking spaces may be provided for the following categories:

- NIST Executive spaces (Director (1); Associate Directors (1 each); Organizational Units (2 each); Chief Officers (1 each);
- Federal Government Vehicles;
- Health Care;
- Special Permit/Disabled;
- Time Limited (loading/unloading, 30-minute visitor parking, etc.);
- Type of Vehicle (compact cars, motorcycles, etc.);
- Combined Federal Campaign (CFC) parking; and
- Other designated spots as approved herein.

Reserved Carpool Parking Spaces

- Reserved parking spaces are provided for registered carpools.
- To register for a reserved carpool parking space, a Carpool Representative must be designated for each carpool. The Carpool Representative completes [Form NIST-1289, Carpool Application](#), available from the Badge Office. An individual may be listed on only one carpool application at a time. The Carpool Representative shall immediately report changes in carpool membership to the Badge Office. If carpool membership declines to just one member, that individual must relinquish the mirror-hanger permit to the Badge Office.
- In addition to the regular parking hanger, a mirror-hanger permit for the vehicle's rearview mirror must be displayed while parking in a reserved carpool parking space. Only one nontransferable mirror-hanger permit is issued per carpool and is shared by all members.
- A vehicle displaying both the mirror-hanger permit and the regular parking permit may park in the spaces marked "Reserved Carpool." When driving to work alone carpool members shall not use "Reserved Carpool" spaces.

- e. Administrative action may be taken for misrepresentation of carpool membership, registration qualifications, or for violation of other NIST carpool practices and requirements as defined herein.

Reserved Parking for Visitors

- a. Only visitors may use designated “Visitor” parking spaces in addition to any available unrestricted space.
- b. Visitor parking is limited to the duration of the visit only.

Processing Violations

In processing violations, which include Federal Violation Notices (citation) and Warning Notices, the observing officer should adhere to the following procedures:

- a. When a Federal Violation Notice (citation) is issued, it is sent to the United States Courts. All matters concerning the citation, once issued, including penalties, collateral, and hearing dates, are handled through the United States Court.
- b. When a Warning Notice is issued no penalty applies and the record is maintained within the DOC OSY PSG.
- c. The supervisor of the vehicle owner/operator may be notified of any violations.

Overnight Parking on the NIST Grounds

NIST employees/associates and visitors who leave the Gaithersburg Campus but need to leave their personal vehicle on the grounds overnight must notify the DOC OSY PSG in advance and park only in areas designated by DOC OSY PSG. NIST employees/associates who leave a vehicle on site while on travel must park their vehicles in the designated long term parking area. A personal vehicle may be parked on the grounds for not more than two weeks unless the vehicle owner presents DOC OSY PSG with a copy of official travel orders indicating that his or her absence will extend beyond two weeks.

During snow emergencies, NIST employees/associates who leave their vehicles on the NIST site overnight are requested to park in the designated long term parking areas. This enables the Plant Division to remove snow and ice from parking lots and reduces the possibility of blocking in or damaging those vehicles.

DIRECTIVE OWNER

137 – Emergency Services Office, ESO

APPENDICES

Appendix A: Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Ver. 2 Draft	10/8/2016	Ed Mai	Updated to ESO as Directive Owner
Ver. 2.0	10/12/2016 3	Dan Cipra	Incorporated changes

Transit Subsidy Program

NIST PR 2106.02

Effective Date: 5/11/2016

PURPOSE

This directive establishes procedures for the Transit Subsidy Program and the Transit Benefits for Bicyclists, including responsibilities, and details outlining the specifics of the program.

APPLICABILITY

This directive is applicable to all full-time NIST employees. Others are not eligible to participate in this program, though the employers of associates may offer similar benefits.

REFERENCES

- [Executive Order 12191 – Federal Facility Ridesharing Program of February 1, 1980](#)
- [Executive Order 13150](#) of April 21, 2000 – Federal Workforce Transportation
- [Title 26, U.S.C., Section 132\(f\)](#) - Qualified Transportation Fringe
- [Federal Employees Clean Air Incentives Act of 1993](#)
- [OPM Decision Letter S001842 dated August 11, 1998](#)
- [Department Administrative Order 217-8 “Employee Parking, Ridesharing, and Mass Transit Benefit Program”](#)
- [IRS Publication 15-B “Employer’s Tax Guide Fringe Benefits”](#) – for current tax year
- [U.S. Department of Commerce Transit Benefits for Bicyclists](#)
- [O 2106.00 Transportation Program](#)
- [NIST-1295, Federal Workforce Transportation Subsidy Application](#)

DEFINITIONS

Employee – for this purpose of this program, employee is defined as an individual who is: (1) employed by NIST; and (2) paid through the National Finance Center (NFC).

RESPONSIBILITIES

Office of the Chief Facilities Management Officer is responsible for:

- The maintenance of all records of this program
- Review and approval of the procedures and guidelines at each NIST site

- Receipt and review of monthly accountability reports and consolidated quarterly reports
- Receipt and review of annual report and any required response to address internal control and/or other issues
- Preparation of any NIST-wide consolidated report that may be required
- Authorization to funds expenditure for the purchase of fare media

Local Transit Subsidy Program Coordinator is responsible for:

- Approval and processing of Transit Subsidy Program and Transit Benefits for Bicyclists forms
- Maintenance of a recordkeeping database
- Ensuring participants do not receive both transit and bicycle benefits
- Purchase and distribution of fare media
- Delivery of participating [SF-1164](#) forms with receipts to Accounts Payable for employee reimbursement for bicycle benefits
- Billing participating Organizational Units (OUs)
- Reducing monthly fare based on participant notification of absences and request of change (as applicable to the fare media program)
- Preparation of reports as required by the Department of Commerce, Department of Transportation, and other government entities
- Making arrangements for investigation of alleged misuse, abuse or fraud, and initiating appropriate corrective action
- Providing guidance and assistance to program participants

Supervisors are responsible for:

- Review and approval of applications to certify participant eligibility for program participation and annual recertifications as necessary
- Initiating an investigation of participants upon suspicion that the subsidy is not being used in accordance with the program parameters
- Ensuring that the participant transit benefits form is completed for annual recertification
- Ensuring that the transit benefits form is completed in conjunction with separation and clearance procedures to withdraw the employee from the program when leaving NIST

Administrative Officers (AOs) are responsible for:

- Providing, upon request, project-task information and authorization for payment to the Facilities Services Division for participants in their supported organizational area

Participating employees are responsible for:

- Completing forms as required
- Complying with the parameters for the program as described in the site-specific procedures

PROCEDURES

The procedures for participation in the program vary by location. The appendices provide the details as to application and eligibility for participation.

Appendix A - Transit Subsidy Program Procedures for Gaithersburg Site

Appendix B - Transit Subsidy Program Procedure for Boulder Site

Appendix C - Transit Benefits for Bicyclists Program Procedures

DIRECTIVE OWNER

190 - Office of Chief Facilities Management Officer

APPENDICES

A. Transit Subsidy Program Procedures for Gaithersburg Site

B. Transit Subsidy Program Procedure for Boulder Site

C. Transit Benefits for Bicyclists Program Procedures

D. Revision History

APPENDIX A

TRANSIT SUBSIDY PROGRAM PROCEDURES FOR GAITHERSBURG SITE

LOCAL TRANSIT SUBSIDY PROGRAM COORDINATOR –

For the Gaithersburg site, the program coordinator is the Chief Facilities Management Officer's Facilities Services Division Transit Point of Contact.

ELIGIBILITY

Participants must be full-time NIST employees with a valid NIST Identification Card and Building Pass.

Participants must use approved mass transportation at least three days per week in lieu of a single occupancy vehicle (SOV) to commute between work and home.

Approved mass transportation includes:

- **RAIL** - Metrorail, MARC Train
- **BUS** - Metrobus, MTA, Eyre Bus Service, Fairfax Connector, DASH, OMNI Ride, and Montgomery County Division of Transit Services (Ride On)
- **OTHER** - Vanpool (Commuter Highway Vehicle) defined as having a seating capacity of at least six plus a driver, the number of occupants being transported must be at least 50 percent of the seating capacity excluding the driver, and 80 percent of vehicle mileage must be accumulated between the residence and the work station

RESPONSIBILITIES

Participating employees are responsible for:

- Filing Form [NIST-1295](#), Federal Workforce Transportation Application, with accurate information and all required signatures for participation, modifications, withdrawals, and annual recertification
- Immediately reporting to the program administrator, by submission of an updated NIST-1295, any change in mode of transportation, residence, commuting cost, work schedule (including telecommuting), or employment status which renders participant ineligible
- Fare media upon receipt (lost, stolen, or misplaced transit benefits are not replaced)
- Any exchange of fare media through online accounts that is necessary
- Ensuring that subsidy is used only for commuting to and from work, not parking, by the participant to which it was issued

PROCEDURES

- a) Approved participants receive a subsidy in the form of an electronic SmartBenefits' funds transfer to their SmarTrip card, which will be approximately equal to but not exceed the employee's commuting cost excluding parking fees. The amount will not exceed the monthly dollar limit set by the Internal Revenue Service ([Publication 15-B](#), Employer's Tax Guide to Fringe Benefits). "Approximately equal to" is defined as to the nearest \$1.00.
- b) SmartBenefits need to be exchanged for acceptable media with transit providers (MARC, Eyre, etc.). This shall be done through Washington Metro Area Transit Authority (WMATA) and CommuterDirect websites. Specific instructions are provided by the Transit Point of Contact upon the enrollment of a participant in SmartBenefits.
- c) Transit subsidy is automatically deposited on enrolled SmarTrip cards, registered to a participant, on the first of each month. Funds are reduced as the card is used on public transportation, or exchanged online for appropriate transit passes.
- d) The above steps must all be met before the 15th of the month prior to when the receipt of electronic benefits and tickets is to start.
- e) Participants shall recertify their eligibility on an annual basis, as required by the Department of Commerce, through completion and submission of Form NIST-1295, Federal Workforce Transportation Application, to the Office of the Chief Facilities Management Officer's Facilities Services Division Transit Point of Contact not later than May each calendar year.

APPENDIX B

TRANSIT SUBSIDY PROGRAM PROCEDURES FOR BOULDER SITE

LOCAL TRANSIT SUBSIDY PROGRAM COORDINATOR –

For the Boulder site, program coordinator is located in the Boulder Facilities Maintenance Division.

ELIGIBILITY

Participants must be full-time NIST employees with a valid NIST Identification Card and Building Pass.

Participants must use approved public transportation at least three days per week in lieu of a single occupancy vehicle (SOV) to commute between work and home.

Approved mass transportation includes:

- **EcoPass** – An annual photo I.D. transit pass. It provides unlimited rides on Local, Regional, and Airport anywhere within the Regional Transit District (RTD) fixed-route system
- **Vanpool** (Commuter Highway Vehicle) defined as having a seating capacity of six plus a driver, the number of occupants being transported must be at least 50 percent of the seating capacity excluding the driver, and 80 percent of vehicle mileage must be accumulated between the residence and the work station

ECOPASS PROGRAM

To participate in the EcoPass program, the Department of Commerce Laboratories (NIST, NOAA and NTIA) must purchase a number of EcoPasses equal to the number of full-time federal employees on the site. The Department of Transportation makes a determination that the program is more cost effective than the purchase of RTD FlexPasses program for only those employees in the transit subsidy program. The deeply discounted EcoPasses have proven to be more cost-effective option for the laboratories.

NIST computes the number of employees who apply for the EcoPass and divide the cost of all EcoPasses by that number, the value derived is the amount billed for the EcoPasses which are distributed. Even though each organizational unit is billed for an amount higher than the “face value” of the EcoPass, the amount is lower than the cost they would incur using the FlexPass.

To be eligible for participation in the EcoPass program, NIST staff must commit to using the RTD system for 8 months during the calendar year.

In 2013, RTD transitioned from a sticker affixed to the NIST Badge holder to a RTD Smart Card.

RESPONSIBILITIES

Participating employees are responsible for:

- Filing the appropriate application for transit benefits, with accurate information and all required signatures for participation, modifications, withdrawals, and annual recertification
- Participants are required to produce a valid Form NIST-458, NIST ID Card/Pass, at time of receipt of subsidy benefits
- Pickup of an RTD Smart Card which involves getting your picture taken and transferred to the media
- The RTD Smart Card will remain the property of the individual. If lost, stolen or misplaced the participant must immediately notify the Local Transit Subsidy Program Manager so that the card can be deactivated. The participant must then make arrangements for a replacement RTD Smart Card
- Immediately reporting to the program administrator, by submission of an updated application for transit benefits, any change in mode of transportation, residence, commuting cost, work schedule (including telecommuting) or employment status which renders participant ineligible
- Immediately reporting to the program administrator any absences from work which would result in a reduction in commuting cost where the subsidy issued for the month exceeds/ed the participant's actual expenses for the month
- Any exchange of fare media that is necessary
- Ensuring that subsidy is used in accordance with program parameters

PROCEDURES

- a) Approved participants receive a subsidy in the form of a RTD Smart Card with the associated privileges of the EcoPass.
 - The cost of the benefit will vary from year to year.
 - The Employee must complete the appropriate application for transit benefits to show monthly commuting costs. NIST transit subsidy cannot exceed the employee's commuting cost excluding monthly parking fees, in accordance with the dollar limit set by the Internal Revenue Service ([Publication 15-B](#) (2009), Employer's Tax Guide to Fringe Benefits). "Approximately equal to" is defined as to the nearest \$1.00.
 - The Employee must show how many months he/she will use RTD as his/her regular mode of transportation to qualify for the benefit.

- b) Supervisors will review the form and the estimates to ensure the eligibility of the participant for the program and that the employee is not provided a benefit exceeding that permitted by the IRS.
- c) Participants shall recertify their eligibility on an annual basis, as required by the Department of Commerce, through completion and submission of the appropriate application for transit benefits, to the Office of the Chief Facilities Management Officer via the Local Transit Subsidy Coordinator no later than September of each calendar year. This verification will be used to determine the cost effectiveness of the EcoPass versus FlexPass programs.
- d) Upon determination of the program to be used, the Local Transit Subsidy Coordinator will inform all NIST Boulder Administrative Officers of the estimated cost of the EcoPass program per participant for the upcoming calendar year.
- e) In August, the Local Transit Subsidy Program Coordinator will invoice each OU for the number of EcoPasses used by their employees.

VANPOOL PROGRAM

RESPONSIBILITIES

Participating employees are responsible for:

- Filing the appropriate application for transit benefits, with accurate information and all required signatures for participation
- Pickup of approved subsidy from the Boulder Maintenance and Support Services Division not later than the 10th workday of each participating month. Workdays are defined as Monday through Friday, excluding federal holidays. Participants are required to produce a valid Form NIST-458, NIST ID Card/Pass, at time of receipt of subsidy benefits
- Ensuring that subsidy is used in accordance with program parameters

PROCEDURES

- a) Approved participants receive a subsidy in the form of an EcoPass or payment vouchers.
- b) Payment Vouchers are received on a monthly basis in the Boulder Maintenance and Support Services Division office.
- c) Payment Vouchers shall be exchanged for acceptable media with transit providers, i.e., Way to Go (Denver Metro Area), VanGo (North Front Range) and Mountain Metro Rides (Colorado Springs).
- d) Participants shall recertify their eligibility on an annual basis, through the completion of the transit benefits application form and worksheet received annually from the Local Transit Subsidy Coordinator via email.

APPENDIX C

TRANSIT BENEFITS FOR BICYCLISTS PROGRAM PROCEDURES

LOCAL TRANSIT SUBSIDY PROGRAM COORDINATOR –

The program coordinator is the Chief Facilities Management Officer's Facilities Services Division Transit Point of Contact(s).

ELIGIBILITY

Participants must be full-time NIST employees with a valid NIST Identification Card and Building Pass. Participants must regularly use a non-motorized bicycle for a substantial portion, 50 percent or greater, of the travel between their residence and the worksite.

Reimbursable bicycle commuting costs under this program may include the purchase of a bicycle, lock, parking/storage, parts, rentals, repairs, and general maintenance.

RESPONSIBILITIES

Participating employees are responsible for:

- Preparation and submission of the U.S. Department of Commerce Request for Bicycle Commuter Subsidy to the appropriate Transit Point of Contact for establishment of participation in the program each year
- Preparation and submission of form [SF-1164](#) Claim for Reimbursement for Expenditures on Official Business and receipts to the appropriate Transit Point of Contact no later than the 15th of each month for request of reimbursement of costs up to \$20, not to exceed \$240 in a calendar year
- Ensuring their claimed reimbursements are accurate and that they do not receive any other Federal employee transit or parking subsidies during the month the bicycle benefit is claimed

PROCEDURES

- a) Participants must complete and have signed the U.S. Department of Commerce Request for Bicycle Commuter Subsidy form, and submit it to the appropriate Transit Benefit Coordinator for enrollment as a participant of the program each calendar year.
- b) Participants must, by the 15th of each month, complete and have signed the [SF-1164](#) Claim for Reimbursement for Expenditures on Official Business form, as instructed below:
 - In Section 1. Please enter NIST and your division, or equivalent, number
 - Do NOT complete Sections 2. or 3

- Only parts (a), (c) and (d) are required for Section 4. The mailing address in part (c) should be your office address, not home
 - Under Section 6. Complete the last two numbers for the date, enter “C” in part (b) for the code, use part (c) as the description of the purchase, and enter the cost (up to \$20 each month) in part (i)
 - Enter the total of all claimed purchases in Section 7. under column (i) (not to exceed \$20)
 - Your Supervisor must sign and date Section 8
 - You must sign and date Section 10
 - The Administrative Officer (AO) must add the project-task and organizational code information at the bottom of the form under “Accounting Classification”
- c) Attach all receipts for the claimed purchase(s) to the completed [SF-1164](#) form, keeping copies of the receipts for your reference, and submit the whole package to the appropriate NIST Transit Benefits Coordinator

If the total cost of a qualified purchase exceeds \$20, it is the participant’s responsibility to submit a new [SF-1164](#) each month until the total cost is paid (not to exceed \$240 annual total).

APPENDIX D

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	12/3/2015	Krista Faecke	Initial Draft
Rev. .01	1/29/2016	Dan Cipra	Formatting Updates
Rev. .02	2/16/2016	Krista Faecke	Add O 2106.00 to references section
Rev. .03	4/4/2016	Dan Cipra	Added links and formatting
Rev. .04	5/5/2016	Krista Faecke	Incorporated all DRB Review comments

Bicycle Parking Notice

NIST N 2106.01
Effective Date: 4/30/2015

PURPOSE

The purpose of this notice is to facilitate the management of bicycle parking on NIST sites and enable optimum use of available bicycle parking spaces at NIST.

This notice that will be in effect until it is replaced with a Procedure directive.

APPLICABILITY

This directive is applicable to all NIST employees and Associates to the extent allowed by law and the terms of the Associate's agreement.

REQUIREMENTS

- Persons need not obtain a NIST Parking Permit for a bicycle.
- The **only** areas designated for bicycle parking are bicycle racks and day use bicycle lockers. Persons must obtain the written authorization of the NIST Police Services Group to park a bicycle in a designated area on the NIST campus for longer than 24 consecutive hours. NIST Police Services Group will maintain a listing of owners who self-identify their bicycles. Persons may not park, secure, or store bicycles at any other location on the campus, including railings, light posts or signposts of any kind. .
- Bicycle racks and day use bicycle lockers are available on a first come, first served basis, and are not assigned to individuals.
- Bicycles are not permitted inside NIST buildings in accordance with 15 CFR §265.22

PROCEDURES

Unless an exception has been obtained in writing from the NIST Police Services Group, bicycles parked at bicycle racks or stored in day use bicycle lockers in excess of 24 consecutive hours, OR parked at any location other than a bicycle rack or day use bicycle locker, will be tagged with a notification. The notification will state that if the bicycle is not removed from the rack or the day use bicycle locker within five consecutive calendar days from the date of the notification, the bicycle will be removed and impounded by the NIST Police Services Group.

Bicycles that have been tagged and continue to remain on the bicycle rack or in the day use bicycle locker for five consecutive calendar days after the date of the notification will be

considered abandoned and therefore, removed and impounded by the NIST Police Services Group for a period of thirty (30) calendar days.

Any lock securing an impounded bicycle will be broken to remove the bicycle from the bicycle rack or day use bicycle locker. NIST will not replace the lock or reimburse the owner for the cost of the lock.

Owners may reclaim their impounded bicycles by contacting the NIST Police Services Group within thirty (30) calendar days of the removal. Owners will be required to sign an affidavit of ownership, criminal penalties may be charged for false statements. At the end of the month, at least 30 days after impoundment, NIST will discard the impounded bicycles.

DIRECTIVE OWNER

Chief, NIST Emergency Services Division

APPENDICES

Appendix A – Sample Tag for Bicycle Violation

Appendix B – Sample Tag to Authorize Extended Storage

Appendix C – Revision History

Appendix A

SAMPLE TAG FOR BICYCLE VIOLATION

NIST Police Services Group (PSG) BICYCLE NOTIFICATION

This bicycle is tagged for the following reasons:

☐ **Parked or stored in excess of 24 hours;**

This bicycle has been parked at this location in excess of 24 hours without being moved. Failure to claim and/or remove this bicycle within 5 calendar days of this notification will lead to the bicycle's removal, impoundment, and possible disposal by the NIST PSG.

☐ **Parked or stored at an unauthorized location.**

This bicycle has been parked or stored at an unauthorized location. Bicycles must be parked in designated areas on the NIST campus, and may not be parked or stored inside a NIST building. The only areas designated for bicycle parking are bicycle racks and day use bicycle lockers.

If this bicycle is not moved from this location before the date shown below, it will be deemed Voluntarily Abandoned Property and will be removed and impounded by NIST PSG. **If the bicycle is not claimed within 30 days after removal, the bicycle will be destroyed. The owner is responsible for contacting NIST PSG at (301) 975-2805.**

Report Number: _____

Notice Date: _____

Removal Date: _____

Issuing NIST Police Officer: _____

This notification is issued in accordance with NIST N XXXX.XX Bicycle Parking Notice.

Appendix B

SAMPLE TAG TO AUTHORIZE EXTENDED STORAGE

NIST Police Services Group (PSG) BICYCLE EXTENDED STORAGE AUTHORIZATION

**THE OWNER OF THIS BICYCLE HAS REQUESTED AUTHORIZATION FOR EXTENDED
STORAGE BASED UPON:**

- ☐ **OFFICIAL TRAVEL**
- ☐ **OTHER*** _____

**THIS BICYCLE HAS BEEN AUTHORIZED TO REMAIN STORED ON THE NIST CAMPUS, IN
A BICYCLE RACK OR LOCKER UNTIL:**

DATE: _____

**FAILURE TO REMOVE THE BICYCLE AFTER THIS DATE WILL RESULT IN A NOTICE
AND POSSIBLE IMPOUNDMENT AND DISPOSAL OF THE BICYCLE.**

Report Number: _____

Authorization Date: _____

Issuing NIST Police Officer: _____

Questions should be referred to the NIST PSG at (301) 975-2805.

**PSG will approved "other" reasons for extended storage on a case-by-case basis.*

Appendix C

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial		Ed Mai	
Rev. .01	3/30/2015	Dan Cipra	Formatting updates

Energy and Sustainability Management Program

NIST O 2107.00

Effective Date: 2/2/2016

1. PURPOSE

This order establishes requirements, responsibilities, and authorities necessary to achieve the goals established to strengthen Federal leadership for sustainable operations of facilities and activities as prescribed by statutes, Presidential Executive Orders, and Department of Commerce and other federal directives for energy and environmental management. To the extent that the term sustainability encompasses other programs that relate to environmental stewardship that are traditionally managed by other Chief Offices, this order does not supersede existing guidance. Rather this order is meant to work in concert with existing programs and directs the Organizational Units (OU) and Chief Offices to collaborate across all programs related to or affecting sustainability.

2. APPLICABILITY

This order applies to all NIST owned and operated sites (Gaithersburg, Boulder, Ft. Collins and Kauai) and all site occupants including NIST employees and Associates to the extent allowed by law and the terms of the Associates' agreement with NIST, or agreements with non-NIST entities.

3. AUTHORITIES AND REFERENCES

- [Energy Policy Act of 2005, August 8, 2005 \(EPAct 2005\)](#)
- [Energy Independence and Security Act of 2007 \(EISA 2007\), December 19, 2007](#)
- [Emergency Planning and Community Right to Know Act of 1986, October 17, 1986 \(EPCRA Act of 1986\)](#)
- [Executive Order No. \(EO\)13693 - Planning for Federal Sustainability in the Next Decade \(March 19, 2015\)](#)
- [Energy and Environmental Management, Department Administrative Order \(DAO 217-16\), April 3, 2012](#)
- [Department of Commerce Real Property Management Manual, August 2014, and subsequent revisions](#)
- [Department of Commerce Strategic Sustainability Performance Plan, June 2013 and future revisions](#)
- [Implementation Handbook for the Strategic Sustainability Performance Plan, August 2013 and subsequent revisions](#)
- [Federal Leadership in High Performance and Sustainability Buildings Memorandum of Understanding](#)

- [Guiding Principles for Federal Leadership in High Performance and Sustainable Buildings \(2008\) \(Guiding Principles\)](#)
- [NIST Order O 7301.00, Environmental Management](#) (11/5/2014)

4. DEFINITIONS

Alternative energy – energy generated from technologies and approaches that advance renewable heat sources, including biomass, solar thermal, geothermal, waste heat, and renewable combined heat and power processes; combined heat and power; small modular nuclear reactor technologies; fuel cell energy systems; and energy generation where active capture and storage of carbon dioxide emissions associated with that energy generation is verified.

Clean energy – renewable electric energy and alternative energy.

Climate-resilient design – to design assets to prepare for, withstand, respond to, or quickly recover from disruptions due to severe weather events and climate change for the intended life of the asset.

Combined Heat and Power (CHP) – sometimes called cogeneration – an efficient, clean method of generating electric power and useful thermal energy (heat) from a single fuel source at the point of use. Instead of purchasing electricity from the local utility company and burning fuel in an on-site boiler to produce needed thermal energy, CHP can provide both energy services in one energy efficient step. CHP can provide significant energy efficiency and environmental advantages over separate heat and power – less fuel is consumed and greenhouse gases (GHGs) and other emissions are reduced.

Greenhouse gases (GHG) – carbon dioxide, methane, nitrous oxide, hydrofluorocarbons, perfluorocarbons, nitrogen trifluoride, and sulfur hexafluoride.

Guiding Principles for Federal Leadership in High Performance and Sustainable Buildings (Guiding Principles, in short) – a set of established criteria developed by the U.S. Government for use by federal agencies committed to federal leadership in the design, construction, and operation of High-Performance and Sustainable Buildings. The Guiding Principles are: Employ Integrated Design Principles, Optimize Energy Performance, Protect and Conserve Water, Enhance Indoor Environmental Quality, and Reduce Environmental Impact of Materials. (*See Guiding Principles.*)

Net-zero energy building – an energy-efficient building where, on a source energy basis, the actual annual delivered energy is less than or equal to the on-site renewable exported energy.

Net-zero water building – a building that is designed, constructed, or renovated and operated to greatly reduce total water consumption, use non-potable sources as much as possible, and recycle and reuse water in order to return the equivalent amount of water as was withdrawn from all sources, including municipal supply, without compromising groundwater and surface water quantity or quality.

Net-zero waste building – a building that is operated to reduce, reuse, recycle, compost, or recover solid waste streams (with the exception of hazardous waste), thereby resulting in zero waste disposal.

Power usage effectiveness – the ratio obtained by dividing the total amount of electricity and other power consumed in running a data center by the power consumed by the information and communications technology in the data center.

Renewable energy certificate (REC) – the technology and environmental (non-energy) attributes that represent proof that 1 megawatt-hour (MW) of electricity was generated from an eligible renewable energy resource, that can be sold separately from the underlying generic electricity with which they are associated and were produced by sources of renewable energy placed into service within 10 years prior to the start of the fiscal year (FY) .

Renewable electric energy – energy produced by solar, wind, biomass, landfill gas, ocean (including tidal, wave, current, and thermal), geothermal, geothermal heat pumps, microturbines, municipal solid waste, or new hydroelectric generation capacity achieved from increased efficiency or additions of new capacity at an existing hydroelectric project.

Scope 1, 2, and 3 –

Scope 1: direct greenhouse gas emissions from sources that are owned or controlled by the agency.

Scope 2: direct greenhouse gas emissions resulting from the generation of electricity, heat, or steam purchased by an agency.

Scope 3: greenhouse gas emissions from sources not owned or directly controlled by an agency but related to agency activities such as vendor supply chains, delivery and transportation services, and employee travel and commuting.

Sustainability – in a general sense is the capacity to support, maintain or endure. Since the 1980s, human sustainability has been related to the integration of environmental, economic, and social dimensions towards global stewardship and responsible management of resources.

Zero-emission vehicle – a vehicle that produces zero exhaust emissions of any criteria pollutant (or precursor pollutant) or greenhouse gas under any possible operational mode or condition.

5. REQUIREMENTS

EO 13693 states that “all Federal agencies’ first priority should be on reducing energy use and cost, then on finding renewable or alternative energy solutions”. (See EO 13693, section 1 policy, paragraph 2.) Therefore, NIST shall:

Promote building energy conservation, efficiency, and management by:

- Reducing building energy intensity per square foot by 2.5 percent annually through the end of FY 2025, relative to the baseline energy use in FY 2015, and

- Improving data center energy efficiency by installing / monitoring advanced energy meters by FY 2018; and establishing a power usage effectiveness target of 1.2 to 1.4 for new data centers and less than 1.5 for existing data centers.

Ensure that, at a minimum, the following percentages of total building electric energy shall be clean energy, accounted for by renewable electric energy and alternative energy:

- not less than 10 percent in FY 2016 and 2017,
- not less than 13 percent in FY 2018 and 2019,
- not less than 16 percent in FY 2020 and 2021,
- not less than 20 percent in FY 2022 and 2023, and
- not less than 25 percent in FY 2025 and each year thereafter.

Ensure that the percentage of the total amount of building electric energy consumed that is renewable energy is:

- not less than 10 percent in FY 2016 and 2017,
- not less than 15 percent in FY 2018 and 2019,
- not less than 20 percent in FY 2020 and 2021,
- not less than 25 percent in FY 2022 and 2023, and
- not less than 30 percent in FY2025 and each year thereafter.

Pursue renewable electric energy in the following order of priority:

- Install NIST funded renewable energy on site and retain the corresponding RECs or obtain equal value replacement RECs,
- Contract for the purchase of energy that includes installing renewable energy on site or off site and retaining the corresponding RECs or obtaining equal value replacement RECs for the term of the contract,
- Purchase electricity and corresponding RECs or obtain equal value replacement RECs, and
- Purchase RECs.

Include the following actions, where feasible, in the alternative energy portion of the clean energy targets listed above:

- Install thermal renewable energy on site and retain corresponding renewable attributes or obtain equal value replacement RECs where applicable,
- Install combined heat and power processes on site, etc.

Improve water use efficiency and management, including storm water management, by:

- Reducing potable water consumption intensity as measured in gallons per gross square foot by 36 percent by FY 2025 through reductions of 2 percent annually relative to a FY 2007 water consumption baseline,
- Installing water meters and collecting / utilizing building and facility water balance data to improve water consumption and management,

- Reducing industrial, landscaping, and agricultural water consumption measured in gallons by 2 percent annually through FY 2025 relative to an FY 2010 water consumption baseline, and
- Installing appropriate green infrastructure features on federally owned property to help with storm water and wastewater management.

Improve fleet and vehicle efficiency and management by:

- Taking action that reduces fleet-wide per-mile greenhouse gas emissions from fleet vehicles, relative to a baseline of emissions in FY 2014, to achieve the following percentage reductions:
 - not less than 4 percent by the end of FY 2017
 - not less than 15 percent by the end of FY 2021, and
 - not less than 30 percent by the end of FY 2025.
- Collecting and utilizing as a fleet efficiency management tool, as soon as practicable but no later than March 2017, fleet operational data through deployment of vehicle telematics at the vehicle asset level for all new passenger and light duty vehicle acquisitions and for medium duty vehicles where appropriate,
- Ensuring that annual asset-level fleet data is properly and accurately accounted for in a Fleet Management System and any relevant data is submitted to the Federal Automotive Statistical Tool (FAST) reporting database, the Federal Motor Vehicle Registration System, and the Fleet Sustainability Dashboard (FleetDASH) system,
- Planning for fleet composition such that by December 31, 2020, zero emission vehicles or plug-in hybrid vehicles account for 20 percent of all new passenger vehicle acquisitions and by December 31, 2025, zero emission vehicles or plug-in hybrid vehicles account for 50 percent of all new passenger vehicles,
- Planning for appropriate charging or refueling infrastructure or other power storage technologies for zero emission vehicles or plug-in hybrid vehicles and opportunities for ancillary services to support vehicle-to-grid technology, and
- Considering the development of policies to promote sustainable commuting and work-related travel practices for Federal employees that foster workplace vehicle charging, encourage telecommuting, teleconferencing, and reward carpooling and the use of public transportation, where consistent with NIST and Department of Commerce authority and Federal appropriations law.

Improve building efficiency, performance, and management by:

- Achieving a 25% reduction in Scope 1 and 2 greenhouse gas (GHG) emissions by FY 2025 from NIST's FY 2008 baseline of carbon dioxide equivalent emissions,
- Achieving a 9% reduction in Scope 3 GHG emissions by FY 2025 from NIST's FY 2008 baseline of carbon dioxide equivalent emissions,
- Ensuring, beginning in FY 2020 and thereafter, that all new construction of NIST buildings greater than 5,000 gross square feet that enter the planning process are

designed to achieve energy net-zero and, where feasible, water or waste net-zero by FY 2030,

- Achieving at least 15 percent, by number or total square footage, of existing buildings above 5,000 gross square feet that comply with the revised Guiding Principles for Federal Leadership in High Performance and Sustainable Buildings by 2025, and make annual progress toward 100 percent conformance with the Guiding Principles,
- Including in all new lease solicitations over 10,000 rentable square feet:
 - Criteria for energy efficiency either as a required performance specification or as a source selection factor in best-value tradeoff procurements, and
 - Requirements for building lessors to disclose carbon emission or energy consumption data for that portion of the building occupied by the agency that may be provided by the lessor through sub-metering or estimation from pro-rated occupancy data, whichever is more cost-effective,
- Reporting building energy, beginning in FY 2016, as part of the Scope 3 greenhouse gas emissions for newly solicited leases over 10,000 rentable square feet,
- Ensuring that all new construction, major renovation, repair, and alteration of buildings include appropriate design and deployment of fleet charging infrastructure, and
- Including the incorporation of climate-resilient design and management elements into the operation, repair, and renovation of existing buildings and design of new buildings.

Improve sustainable acquisition and procurement by ensuring that each of the following environmental performance and sustainability factors are included to the maximum extent practicable for all applicable procurements in the planning, award, and execution phases of the acquisition:

- Meeting statutory mandates that require purchase preference for recycled content products designated by the Environmental Protection Agency (EPA), energy and water efficient products and services such as ENERGY STAR qualified and Federal Energy Management Program (FEMP)-designated products, and Bio Preferred and bio based designated products designated by the U.S. Department of Agriculture (USDA),
- Purchasing sustainable products and services identified by EPA programs including Significant New Alternative Policy (SNAP) chemicals or other alternatives to ozone-depleting substances, Water Sense certified products and services, Safer Choice labeled products, and Smart Way Transport partners and products,
- Purchasing environmentally preferable products or services that meet or exceed specifications, standards, or labels recommended by EPA that have been determined to assist agencies in meeting their needs and further advance sustainable procurement goals of EO 13693, and

- Reducing copier and printing paper use and acquiring uncoated printing and writing paper containing at least 30 percent postconsumer recycled content or higher as designated by future implementing instructions from the Council on Environmental Quality (CEQ).

Advance waste prevention and pollution by:

- Reporting in accordance with the requirements of sections of 301 through 313 of the EPCRA Act of 1986,
- Diverting at least 50 percent of non-hazardous solid waste, including food and compostable material but not construction and demolition materials and debris, annually, and pursuing opportunities for net-zero waste or additional diversion opportunities,
- Diverting at least 50 percent of non-hazardous construction and demolition materials and debris, and
- Reducing or minimizing the quantity of toxic and hazardous chemicals and materials acquired, used, or disposed of, particularly where such reduction will assist in pursuing greenhouse gas emission reduction targets.

Implement performance contracts for NIST buildings by:

- Utilizing performance contracting as an important tool to help meet identified energy efficiency and management goals while deploying life-cycle cost-effective energy efficiency and clean energy technology and water conservation measures,
- Fulfilling existing performance contracting commitments towards the goal of \$4 billion in Federal performance-based contracts by the end of calendar year 2016, and
- Providing annual targets for performance contracting for energy savings to be implemented in FY 2017 and annually thereafter.

Promote electronics stewardship by establishing, measuring, and reporting by:

- Ensuring procurement preference for environmentally sustainable electronic products,
- Establishing and implementing policies to enable power management, duplex, printing, and other energy-efficient or environmentally sustainable features on all eligible electronic products, and
- Employing environmentally sound practices with respect to disposition of all excess or surplus electronic products.

EISA of 2007:

- NIST shall establish a framework for identifying and inspecting all “covered facilities” that constitute at least 75% of the agency’s facility energy use. NIST shall designate an energy manager for each of these covered facilities, and shall complete comprehensive energy and water evaluations on 25% of the covered facilities each year, so that an evaluation is conducted at each facility at least once every four years.

- NIST shall incorporate the following EISA of 2007 issued performance standards for new building construction and major renovation projects:
 - Reduce fossil fuel generated energy consumption 80% by 2020, 90% by 2025, and 100% by 2030 as compared with energy consumption by a similar building in FY 2003.
 - Apply sustainable design principles to the siting, design, and construction of buildings, and identify a certification system and target level of green buildings.
 - Ensure that 30% of the hot water demand be met with solar hot water equipment, provided it is life-cycle cost-effective.

EPAct of 2005: NIST shall incorporate energy efficiency criteria consistent with ENERGY STAR and FEMP-designated products as per EPAct of 2005 for all procurements involving energy consuming products and systems, including guide specifications, project specifications, and construction, renovation, and service contracts that include provisions for energy consuming products and systems.

Metering: NIST shall install advanced meters in all applicable buildings as follows:

- Electric meters as per EPAct of 2005 were due by October 1, 2012.
- Natural gas and steam meters as per EISA 2007 by October 1, 2016.
- Water meters as per EO 13693, without specifying a date.

6. RESPONSIBILITIES AND AUTHORITIES

The NIST Director shall:

- Provide strategic direction and oversight for the NIST Energy and Sustainability Management program and ensure the organizational goals for NIST as delineated in the Requirements Section are achieved, and
- Ensure resources necessary to achieve the program goals are identified and budgeted for in the annual NIST appropriation request to the Department of Commerce.

The Associate Director for Management Resources (ADMR) shall:

- Provide support and oversight of the NIST Energy and Sustainability Management program,
- In conjunction with the Chief Facilities Management Officer, prepare annual budget requests sufficient to meet program goals, and
- Coordinate support within the ADMR organization and Chief Offices for the NIST Energy and Sustainability Management program.

Chief Facilities Management Officer (CFMO):

- Is designated the Chief Sustainability Officer for NIST,
- Shall submit reports twice annually to the Department of Commerce on NIST's progress towards the NIST Energy and Sustainability Management program and organizational goals, and
- Shall be responsible for addressing the following goals and partnering with OU Directors and site occupants to achieve these goals:

- Promoting building energy conservation through the reduction of building energy intensity, and installing meters to facilitate measurement of progress,
- Pursuing and employing clean energy, renewable energy, and alternative energy,
- Improving sustainability and energy efficiency for both owned (greater than 5,000 gsf) and leased (greater than 10,000 rentable sf) buildings and spaces,
- Phasing in building designs that achieve “net-zero” (energy, water, and/or waste), where feasible,
- Performing comprehensive energy and water evaluations on covered facilities,
- Improving water use efficiency and management,
- Improving fleet and vehicle efficiency and management,
- Entering monthly energy and water consumption performance data into the EPA ENERGY STAR Portfolio Manager for all buildings, and
- Continuing to support the use of the NIST Environmental Management System (EMS) as defined in NIST Order O 7301.00 (Environmental Management) and NIST Environmental Management System (EMS). More specifically,
 - Developing Environmental Management Plans (EMPs) to achieve the established goals that include utility efficiency (electric energy and water), fleet vehicles/petroleum conservation/ alternative fuel use, building sustainability, etc.,
 - Assigning EMP Managers to the EMPs for which OFPM is responsible to implement and ensuring that the EMP Managers carry out the EMP by tracking progress through the NIST EMS, and
 - Ensuring EMP Managers serve as members of the NIST Environmental Management Committee at least through completion of their assigned EMPs.

Organizational Unit (OU) and Office Directors:

- Are responsible for assisting the NIST Director and the CFMO in achieving the goals set forth by EO 13693.
- With respect to achieving the goals in this order, OU Directors are responsible for:
 - Being aware of the goals and the EMPs established to achieve the goals,
 - Reviewing practices and activities within their organization to ensure these activities support the plans to the best of their ability,
 - Supporting the CFMO with addressing waste prevention and pollution goals,
 - Engaging and challenging their division chiefs and staff to improve their processes and actions to support NIST’s energy conservation and sustainability goals, and
 - Bringing opportunities for energy conservation and facility sustainability improvements to the CFMO’s attention, to include:
 - a. Requesting CFMO to assess current lab equipment and processes when suspected of possible wasteful energy practices,
 - b. Having planned lab equipment purchases reviewed first by CFMO (i.e., early on in the planning phase, well before the purchase of any equipment so

applicable energy efficient requirements can be inserted in the specifications) to evaluate them for most energy efficient before submitting related procurement action to AMD, and

c. Eliminating single-use pass through of water for cooling of experiments, etc.

Director, Office of Acquisition and Agreements Management: In addition to the responsibilities placed upon all OU and Office Directors, shall

- Address the sustainable acquisition and procurement goals, and
- Promote partnering between contracting officer, purchase card holders, and NIST consumers/users of these products to achieve the goals.

Director, Office of Human Resources Management and Chief Safety Officer: In addition to the responsibilities placed upon all OU and Office Directors, shall:

- Address the GHG Scope 3 emissions reduction goal (i.e., reduce vehicle miles that NIST employees commute to / from work by increasing the use of carpooling, mass transit, and teleworking), and
- Partner with site occupants to achieve the goal.

Chief Safety Officer: In addition to the responsibilities placed upon all OU and Office Directors, shall:

- Support the CFMO with addressing waste prevention and pollution goals,
- Partner with site occupants to achieve these goals, and
- As the NIST Environmental Manager (defined in NIST O 7301.00), ensure that progress towards meeting sustainability goals is tracked through the NIST EMS.

Chief Information Officer: In addition to the responsibilities placed upon all OU Directors, shall:

- Improve data center energy efficiency
- Partner with OU Directors and fellow Chief Officers and Office Directors to address the electronic stewardship goals.

All Supervisors

With respect to the goals in this order, all supervisors shall:

- Maintain awareness of the goals of this program and support all efforts to achieve the goals, and
- Support their OU or Office Director in his/her responsibilities regarding energy and sustainability management.

7. DIRECTIVE OWNER

190 – Chief Facilities Management Officer

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	10/18/2015	Virginia Holtzman-Bell	Initial Draft
Rev. 1	11/4/2015	Dan Cipra	Formatting Updates
Rev. 2	11/5/2015	John Bollinger	Addition of definitions of certain terms, consolidation of OU Director responsibilities into one section
Rev. 3	12/20/2015	John Bollinger	Addressed comments provided by OSHE
Rev. 4	12/23/2015	John Bollinger	Addressed comments provided by NCNR
Rev. 5	1/25/2016	John Bollinger	Addressed comments provided by DRB
Rev. 6	3/23/2016	John Bollinger	Addressed interim comments provided by OCC

Export Control Management Program

NIST O 2108.00

Effective Date: 8/27/2015

PURPOSE

The purpose of this program order is to delineate management and staff responsibilities to identify and safeguard materiel and technology in a manner to prevent violation of export control rules and regulations, that is, to prevent unauthorized exports (including deemed exports) to foreign nationals. This program order establishes requirements, responsibilities, and authorities to safeguard commodities, software, and technology subject to export control rules and regulations.

APPLICABILITY

This order applies to all NIST organizations, employees, and associates to the extent allowed by law and the terms of an associate's agreement.

This order applies to all NIST-administered sites, including those in Maryland, Colorado, and Hawaii.

REFERENCES

This order complies with and implements applicable Department Administrative Orders (DAOs) and Department of Commerce (DOC) regulations involving export control, and in addition it addresses other Federal regulations involving export control, including but not limited to:

- [Export Administration Regulations \(EAR\), 15 C.F.R. Parts 730–774](#)
- [The United States Munitions List, 22 C.F.R. Part 121](#)
- [Nuclear Regulatory Commission \(NRC\) export licensing authority, 10 C.F.R. 110.8 and 110.9](#)
- [Department of Commerce, Department Administrative Order \(DAO\) 207-12, Foreign National Visitor and Guest Access Program](#)
- [Department of Commerce Manual of Security, Policy and Procedures](#)

BACKGROUND

NIST values the contributions of international collaborations to the scientific and technological strength of the United States and to NIST mission success, and offers foreign national visitors and guests access to NIST's facilities, staff, and information to participate in a broad range of activities to include development of international standards. Meetings with and visits by foreign

nationals are common means to facilitate interchange with international scientific and technical counterparts in support of broad agency objectives and program goals. However, NIST must balance this openness with the need to adhere to export rules and regulations.

There are multiple bodies of export regulations that could affect NIST's operations. The regulations that apply most often are the Export Administration Regulations (EAR), which are administered by the Bureau of Industry and Security (BIS) in the Department of Commerce (DOC). In general, the EAR are concerned with "dual use" products and technologies—things that are used for non-military purposes but which have military significance. This program order is principally concerned with the EAR, since these are the regulations with the most direct applicability to the work at NIST. However, in addition, the International Traffic in Arms Regulations (ITAR) control the export of defense-related articles. Nuclear equipment and material are covered by separate regulations, as are exports to nations subject to embargos and sanctions.

DEFINITIONS

The definitions listed below are intended to be consistent with the definitions given in the EAR, Title 15 C.F.R. [§734.2](#), [§772.1](#), and [§774](#). In some cases, the terms within the definitions here are further defined within these sources.

Commerce Control List (CCL) — A taxonomy of items under the export control jurisdiction of the Bureau of Industry and Security, U.S. Department of Commerce. The CCL is found in [Supplement No. 1 to part 774 of the EAR](#). An item described by a CCL entry has a specific Export Control Classification Number (ECCN) assigned to it.

Commodity — Any article, material, or supply except technology and software. This term includes equipment.

Controlled Items — For the purposes of this directive, commodities, software, or technology that are subject to export licensing or other requirements of U.S. export control rules and regulations including, but not limited to, Export Administration Regulations, International Traffic in Arms Regulations, and Nuclear Regulatory Commission (NRC) export licensing authority. Note: a "controlled item" may require an export license unless a license exception applies.

Controlled Technology — For the purposes of this directive, "technology" that is "required" for the development, production, or use of items on the Commerce Control List (CCL). The "technology" for each item on the CCL is controlled according to the provisions in its specification and in its Category (*See* 15 C.F.R. §774, Supplement No. 2). Here, "required" refers to only that portion of "technology" that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions (*See* 15 C.F.R. §772.1). Note: "controlled technology" may require an export license unless a license exception applies.

Deemed Export — Any release of technology or software to a foreign national. Such release is deemed to be an export to the home country or countries of the foreign national. The deemed

export rule does not apply to persons lawfully admitted for permanent residence in the United States and does not apply to persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)). Note that the release of any item to any party with knowledge a violation of the EAR is about to occur is also a violation (*See* 15 C.F.R. §734.2 (b)(2)(ii)). Note that a deemed export is a specific type of export and is included in the scope of the term “export,” where that term is used. Note also that, for the purposes of this directive, the term “deemed export” is meant to be inclusive of a “deemed reexport.” In regulation, this is any release of technology or software to a foreign national in a different foreign nation.

Export — An actual shipment or transmission of items out of the United States, or release of technology or software to a foreign national (*See* 15 C.F.R. §734.2 (b)(1)). For the purposes of this directive, the term “export” is meant to be interpreted broadly. For example, it includes what, in regulation, is called a “reexport”—an actual shipment or transmission of an item subject to U.S. export rules and regulations from one foreign country to another (*See* 15 C.F.R. §734.2 (b)(4)). Note: With few exceptions, NIST-owned property, including non-public information, is subject to U.S. export rules and regulations no matter where it might be in the world.

Export Control Classification Number (ECCN) — A five character alpha-numeric designation used on the Commerce Control List (CCL) to identify an item for export-control purposes. An ECCN categorizes an item based on the nature of the product, i.e. type of commodity, software, or technology, and its respective technical parameters.

Moderate- to High-Risk Equipment — For the purposes of this directive, equipment that, when left unattended, is likely to be covertly inspected and analyzed to determine how it functions, or in the case of equipment that can be used to make dangerous substances or devices, be used for unauthorized purposes.

Property Custodian — Within the NIST Personal Property Management Program, Directive Number O 2102.00, a property custodian is a person responsible for maintaining accountability of all personal property within their assigned area. This responsibility was formerly referred to as being a “Property Officer.”

Property Contact — Within the NIST Personal Property Management Program, Directive Number O 2102.00, the property contact is the person who has day-to-day responsibility for a specific item of property.

Release of Technology or Software — Technology or software is released for export through:

- 1) Visual inspection by foreign nationals of U.S.-origin equipment and facilities;
- 2) Oral exchanges of information in the United States or abroad; or
- 3) The application to situations abroad of personal knowledge or technical experience acquired in the United States (*See* 15 C.F.R. §734.2 (b)(3)).

Software — A collection of one or more “programs” or “microprograms” fixed in any tangible medium of expression. For the purposes of this directive, the term “software” is meant to be

interpreted broadly. It includes, among other things, source code, object (compiled) code, and program fragments, such as subroutines, frameworks, and libraries.

Technology — Specific information necessary for the development, production, or use of a product. The information takes the form of technical data or technical assistance (*See* 15 C.F.R. §772.1). Note: Technology is not necessarily controlled. (*See Controlled Technology, above.*)

Use Technology — Specific information necessary for the use of a product. It consists of information pertaining to: operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing (*See* 15 C.F.R. §772.1).

Notes: This term does not refer to the operation of a product. As a general rule, BIS has determined that all six of these activities must be present to trigger a license requirement for “use technology,” at least with respect to deemed exports (*See* 71 FR 30840–30844, <http://www.gpo.gov/fdsys/pkg/FR-2006-05-31/pdf/E6-8370.pdf>). However, exceptions may arise in future revisions of the CCL and will be covered in training if they do.

REQUIREMENTS AND PRINCIPLES

Duty to Follow Export Regulations:

All persons at NIST-administered sites have a legal responsibility to adhere to export rules and regulations. This means, among other things, that employees, associates, and visitors shall take care to neither export nor allow to be exported any item or technology that requires an export license, unless and until such a license is first obtained. Staff and associates shall take prudent measures to understand the export restrictions of the items and information under their control, and to prevent impermissible deemed exports (releases of software and technology) to foreign nationals. These measures include taking training, as may be offered or required, and following the requirement herein.

Focus of this Program Order and Other, Special Situations:

This program order is principally concerned with satisfying the requirements of the Export Administration Regulations (EAR), since these are the export regulations with the most direct applicability to the work at NIST. However, in addition, managers and staff who may be engaged with articles on the U.S. Munitions List (articles subject to ITAR), radioactive and nuclear material and equipment, and individuals from nations subject to embargos and sanctions should seek individualized guidance from the NIST Office of the Chief Counsel and the Chief of NIST’s Emergency Services Division, as described below.

Applicability of Export Administration Regulations, in General:

Under the EAR, certain commodities, software, and technology require a license (in advance) before they may be exported to certain destinations, entities, and individuals. The scope of exports includes “deemed exports,” by which is meant the release of software or technology to a foreign national person—most often, within the United States. Here, “technology” refers to information rather than physical goods (“commodities”). “Controlled technology” is, in general,

information that enables someone to develop (design), produce (manufacture or replicate), or maintain commodities that meet or exceed the regulatory thresholds that apply to physical exports. Deemed exports occur regardless of the means by which the information is released, be it by oral discussion, visual inspection, access to documents (e.g., plans, blueprints, and service manuals), or other means.

The EAR affect NIST in two distinct ways: in the equipment that we own and in the research that we conduct.

With respect to equipment, the EAR do not regulate the operation of equipment—that is, who is or is not permitted to operate it. However, “use technology” is a type of technology (information) subject to deemed export regulation. It is the information that pertains to: operation, installation, maintenance, repair, overhaul, and refurbishing. BIS has stated that, as a general rule, technology classified as “use technology” must include information pertaining to all six of these activities to trigger a license requirement. With some exceptions, which will be explained during training if they arise, you are generally allowed to disclose to anyone the minimum necessary information to enable the safe operation and routine maintenance of NIST-owned equipment, and to permit them to use it. Nonetheless, there might well be a license required before a foreign national may be taught, or learn from inspection, how NIST-owned equipment is designed, built, or serviced to meet or exceed a regulatory threshold.

With respect to research, the EAR exempt from licensing requirements any information arising during or resulting from “fundamental research.” This means basic and applied research in science and engineering, where the resulting information is ordinarily published and shared broadly within the scientific community. At NIST, research that is undertaken with the unconditional intent to openly publish the results at its conclusion is covered by the fundamental research exemption. The results of research that are not intended for open publication (e.g., because of proprietary interests, security concerns, or any other reason), or which require external approval prior to open publication (e.g., by partners or funding sources), are not covered by this exemption and may require an export license before releasing them or otherwise sharing them with certain foreign nationals. Similarly, the “know how” used to conduct the research is exempt only if it is publicly available information or is intended to be published with the results of the research.

Analyses under the EAR are governed by the specifics of the export: what the item, software, or technology is, where it is going, who will receive it, and what the use is to which it will be put. Analysis begins by classifying the item, software, or technology within a taxonomy called the Commerce Control List (CCL). The result is the determination of an Export Control Classification Number (ECCN). “EAR99” is not an ECCN, but rather a special code meaning that the item, software, or technology falls outside of the specifications of all entries in the CCL. An ECCN specification contains associated requirements for export licenses to certain destinations. However, regardless of the ECCN, licenses are always required for exports to

embargoed or sanctioned countries, to specific parties or institutions of concern, or in support of a prohibited end use (such as nuclear or missile development).

There are five ECCN product groups, as indicated by a letter within each ECCN:

- A. (Systems, Equipment and Components),
- B. (Test, Inspection and Production Equipment),
- C. (Material),
- D. (Software), and
- E. (Technology).

At NIST most inventoried property will have ECCNs in group A or B, or will be designated EAR99. Groups D and E are most frequently involved in discussion of deemed exports.

Inventory:

1. Each item of inventoried equipment has an ECCN (most often in group A or B) or an “EAR99” designation. Property Custodians will work with their Division Chiefs, Group Leaders, and other management and staff as appropriate to enter the current ECCN (or “EAR99”) for all items previously identified as subject to export control within one year of the date this order is implemented.
2. Property Custodians will work with their Division Chiefs, Group Leaders, and other management and staff as appropriate to identify potentially high-risk items not captured in the previous paragraph. Once identified, their ECCNs (or “EAR99”) should be determined and entered into the property database within 30 days.

The ECCN applicable to an item of property may change over time as a result of regulatory changes, and the classification of items within the CCL taxonomy may be uncertain. Therefore, ECCN entries in the property database should be considered advisory rather than authoritative, with further review conducted as might be required, including consulting with the Office of the Chief Counsel for NIST.

Research:

- a. Performance Management Records (Form NIST-01) will be used as the mechanism for determining and recording the disclosure limitations on specific areas of research.

The intent to openly publish the results of research, or not, is decided and documented in the performance plans of the staff performing the research. Such determinations are made jointly between the employee and his/her first-level supervisor. For those areas of work specified under “disclosure authorized,” there are no EAR licensing requirements for the results of the work or for information that arises during such work. For those areas of work specified under “disclosure restricted,” any of a number of considerations (such as the proprietary nature of the work, national security concerns, International Traffic in Arms Regulations (ITAR), Nuclear Regulatory Commission regulations, or external prepublication clearance requirements) may bar public disclosures or disclosures to certain foreign nationals prior to public disclosure. Specific

approval by Division or Laboratory management is required before any information arising during or resulting from such work is disclosed, as per the requirements of the [NIST Technical Communications Program](#). When there are no other restrictions having precedence, an export license may be requested (in advance) to disclose (release) the technology to certain foreign nationals, depending on the ECCN of the technology and the party to receive it.

b. NIST staff must promptly inform their first-level supervisor if they believe that their research should not be openly published, for any reason.

In preparing Form NIST-01, staff should discuss any concerns about the appropriateness of open publication of the research to be undertaken. In addition, staff must promptly notify their first-level supervisor in the event that unanticipated results or concerns arise from research that had previously been designated as “disclosure authorized.” First-level supervisors should seek guidance, as necessary, and decide whether or not to reclassify the research as “disclosure restricted” from that point forward.

Access Controls:

NIST-owned property is subject to risks such as misappropriation (theft), misuse (for other than official, authorized purposes), and safety hazards. In addition, certain property may be attractive for espionage to determine how it achieves or exceeds an export-control threshold. Property contacts and other NIST employees who supervise the use of, or have control over government personal property shall implement prudent and appropriate measures and procedures to mitigate such risks. The ECCN of an item (its technical parameters and the export restrictions arising from it) may be used as an indicator of the potential for industrial espionage. Mitigation strategies commonly employed include locking up such equipment when it is not in use, securing service and technical manuals, and installing controls, such as door locks and alarms that limit access to certain areas to authorized personnel.

Similarly, access controls may be appropriate for areas where research is conducted, if that research is disclosure-restricted.

When access controls are determined to be appropriate, the details should be recorded and shared with staff using the laboratory, managers having responsibility for the laboratory, and the Chief of NIST’s Emergency Services Division. Appendix B illustrates a format that may be used.

Training and Guidance:

a. The Chief Counsel for NIST will ensure training and guidance is provided to OU Directors, Division Chiefs, Group Leaders, and other management, employees, and associates as appropriate to keep them apprised as to current Federal Regulations regarding export controls.

b. The Chief of NIST’s Emergency Services Division will provide training and guidance, on request, for Division Chiefs, Group Leaders, and other management and staff as appropriate on how to provide suitable physical security access controls for “controlled items” and disclosure-restricted research.

Prohibited Practices:

- a. Use of government equipment or equipment loaned to the government for purposes not directly related to official duties.
- b. Removal of equipment from its designated room/building without the specific permission of the responsible property contact or custodian.
- c. Allowing anyone not a Federal employee (including, specifically, foreign national guest researchers) to disassemble or analyze the operation of commercial equipment at NIST in a manner that may be regarded as “reverse engineering”—that is, allowing discovery of non-public information about how the equipment is designed, built, or functions. First-level supervisors may grant exceptions to this general rule when they determine a legitimate programmatic need (e.g., to alter the behavior of the equipment or to interface to it), act to protect the trade secrets of the manufacturer against disclosure outside of the Government, and assure that prohibited deemed exports would not occur. Depending on the nationalities of guest researchers, the ECCNs of the equipment at issue, and the information obtained, an export license may be required (in advance) before guest researchers may acquire the knowledge obtained by such disassembly or analysis.

Note: Repair and maintenance of equipment by its manufacturer or their authorized representative does not constitute reverse engineering. Nonetheless, the use technology made evident by such processes may also require an export license to certain foreign national guest researchers.

Grants and Contracts:

Grantees and contractors are required to comply with EAR requirements (15 C.F.R. Parts 730–774) regarding exports, including deemed exports. NIST grants and contracts entered into, modified, or renewed shall contain the standard clause/term and condition issued by the Office of Acquisition and Agreements Management to address these requirements.

Export Licenses:

The Office of the Chief Counsel for NIST is authorized to apply for export licenses. Requests to initiate export license applications shall be made by memorandum through the Director or Deputy Director of the Organizational Unit (OU) and shall provide all relevant details required for an application and decision. These include, but are not limited to: (1) The item (commodity, software, or technology) at issue, and the regulatory provisions believed to require a license; (2) The extent to which the technology at issue is public, and the extent to which it might be released under the license; (3) The foreign national(s) at issue—who they are, their nationality, and their employer; (4) An explanation of why it is in the Government’s interest to allow the export, including the implications if the license is denied; and (5) How the terms of the export license granted by the Bureau of Industry and Security (BIS) would be enforced. Note: General information on the details required for an export license application may be found on the BIS website.

General guidelines concerning export controls can be found in Appendix A.

RESPONSIBILITIES AND AUTHORITIES

Associate Director for Management Resources (ADMR)

- Accountable for administering the NIST Export Control Management program as described herein, including the policies and procedures required to execute the program.
- Maintaining NIST's property inventory and for including the ECCNs of property as required by this Order.
- Ensuring that adequate security control measures are in place to protect "controlled items" at NIST facilities.
- Assessing compliance with EAR requirements at least once every two years.

Organizational Unit (OU) Director (or Designee)

- Providing oversight to maintain the proper classification of research within the OU as "disclosure authorized" or "disclosure restricted" on NIST-01 (Performance Management Record) forms, and for that research designated as "disclosure restricted," taking necessary measures to prevent unauthorized or inappropriate disclosures.
- Maintaining awareness of the general types of items (including equipment, other commodities, software, and technology) subject to significant export restrictions.
- Ensuring that the property inventory for the OU includes the ECCNs for such items, that appropriate access controls are established and maintained, and that prohibited practices are identified/avoided by members of the organization.
- Approving, with discretion, requests within an OU to apply for export licenses, and forward such requests to the NIST Office of the Chief Counsel.

Division Chief/Group Leader/Other Management and Staff as Appropriate

- Maintaining awareness of the research underway in the organization and the equipment used to conduct it.
- Identifying areas of research that are properly categorized as "disclosure restricted" on NIST-01 (Performance Management Record) forms, and for that research so designated, taking necessary measures to prevent unauthorized or inappropriate disclosures of methods ("know how") or results.
- Maintaining awareness of the general types of items subject to significant export restrictions. All involved should take steps to ensure that the property inventory for the OU includes the ECCNs for such items, that appropriate access controls are established and maintained, and that prohibited practices are identified/avoided by members of the organization.
- Consulting with the Chief of NIST's Emergency Services Division to implement and document access controls.
- Drafting memoranda to the NIST Office of the Chief Counsel requesting applications for export licenses, and route such requests through OU management for approval.

- Completing an annual certification of compliance, as shown in Appendix C. Completed annual certifications will be maintained on file at Division level for two years.

All NIST Researchers (including staff, associates, and guests)

- Abiding by export rules and regulations, and NIST policies, which prohibit exports (including deemed exports) that require a license unless a license is first obtained.
- Not disclosing the methods and results of research that is “disclosure restricted,” except to those authorized to receive it.
- With respect to commercial equipment, not conveying to restricted foreign nationals proprietary technology (information) that is peculiarly¹ responsible for that equipment achieving or exceeding an export-controlled performance level, characteristic, or function, or helping them to obtain export-controlled products.
- Avoiding the Prohibited Practices, above, which may be summarized as:
 - Using Government equipment for non-official or unauthorized purposes,
 - Taking equipment from laboratories without permission, and
 - Allowing anyone not a Federal employee to “reverse engineer” commercial equipment without prior review.
- Taking export control training as might be required.

NIST Office of the Chief Counsel

- Providing training and guidance to Division Chiefs, Group Leaders, and other management and staff as appropriate to keep them apprised as to current Federal regulations regarding protection of proprietary, national security, and other sensitive information. The Office will establish training requirements and schedule training to meet those requirements.
- Acting as the focal point for queries on exports and deemed exports; receiving requests from OUs for export licenses;
- Consulting with Divisions Chiefs to develop the necessary facts to support a determination as to whether or not a license might be necessary and appropriate, and if so, to support a license application.
- Consulting with Bureau of Industry and Security (BIS) and other agencies regarding preparing and submitting formal license applications.

Chief of NIST’s Emergency Services Division

- Assisting Division Chiefs to assess security risks related to “controlled items” in their divisions;
- Assisting Division Chiefs to identify appropriate security control measures to safeguard “controlled items” in their divisions;

¹ See the comment on “Required” found in the definition of “Controlled Technology”

- Providing review and approval of security control procedures and documentation developed by the divisions.

NIST Property Officer

- Maintaining the NIST Property Accountability System.
- Providing training, as needed, for Property Custodians on how to enter ECCN information in the NIST property accountability system.

International and Academic Affairs Office

- Ensuring that any required export licenses and/or necessary approvals are in place prior to approving transactions with foreign entities (e.g. SRM sales);
- Assisting NIST Office of the Chief Counsel with queries on exports and deemed exports with respect to foreign NIST Associates and foreign transactions (e.g. requests for SRMs);
- Reviewing requests from OUs for export licenses for foreign NIST Associates.

DIRECTIVE OWNER

190 - Chief Facilities Management Officer

APPENDICES

- A. General Guidelines
- B. Sample Export Control Procedure Sheet and Factors for Consideration
- C. Sample Annual Certification
- D. Revision History

Appendix A

GENERAL GUIDELINES

If NIST staff operate within the bounds of these General Guidelines, they are unlikely to violate the Export Administration Regulations (EAR).

Operating outside of a General Guideline may or may not require an export license. An analysis of facts and circumstances is necessary. Staff should check with the Office of the Chief Counsel for NIST before proceeding.

Concerning Exports in General:

1. Do not ship or take equipment out of the United States without prior approval. Likewise, do not electronically communicate software or technical know-how. (In other words, before shipping or taking products, production tools, materials, or software out of the United States, or disclosing (releasing) technology outside of the United States, determine whether or not an export license is required. The Office of the Chief Counsel for NIST is available for assistance.)

Concerning Deemed Exports:

1. No export license is required for the results of any research where the unconditional intent exists to publish those results openly. However, do not disclose the results of research indicated in performance plans (NIST-01 forms) as “disclosure restricted” without prior approval.

Caution: As a project progresses, it is possible that a researcher or their supervisor may determine that open publication is no longer appropriate. At that point, foreign national guest researchers must be removed from the project unless analysis determines that the deemed export is allowed without a license or the license is obtained.

2. If a project has pre-publication review requirements (other than NIST editorial review, or a review solely to ensure that publication would not compromise patent rights) or other encumbrances on publication (e.g., proprietary work), foreign nationals should not be included in the project nor briefed on results prior to their public release. (If the right to publish is not unconditional, the fundamental research exemption does not apply until all conditions are met. A separate exemption applies to information once it becomes generally accessible to the public.)
3. No one besides Federal employees should participate in research projects when there is not intent to openly publish the results. (In addition to export regulations, there are other reasons that might preclude participation by non-employees (e.g., NIST Associates), or disclosure of the results. Formal collaborations, of course, specify who is allowed to participate.)

4. Unless advised otherwise in training, no export license is required for the routine operation of any equipment by a foreign national guest or visitor. However, the use of NIST equipment must be limited to Official Government purposes, regardless of who uses it.

Note: Property custodians and contacts (those NIST employees responsible for using or supervising the use of the equipment) should assess the risk that equipment might attract unofficial use (e.g., out of hours) especially if that equipment could be used to make hazardous substances or devices. Moderate- to high-risk equipment should be appropriately secured to avoid such use.

5. Foreign national guest researchers should not be trained in, or perform, non-routine or heavy maintenance of NIST equipment, including skilled repair, overhaul, or refurbishment. (There could be a license required for the deemed export of “use technology.”)
6. Printed or electronic documentation on the design, construction, or heavy maintenance of equipment should be secured.
7. Most commercial equipment at NIST is used “as is” from the manufacturer. On those occasions when NIST staff analyze the inner workings of equipment to modify its operation, to design and implement technical improvements, or to interface that equipment with other equipment, guest researchers—be they domestic or foreign—should not be included in the activity.
8. Property custodians and contacts should assess the risk that equipment, assemblies, and components might attract unauthorized inspection and analysis (e.g., surreptitiously, out of hours). Moderate- to high-risk equipment should be appropriately secured to avoid such inspection and analysis.
9. Property custodians, in consultation with property contacts, should do their best to update the NIST property database with the Export Control Classification Number (ECCN) of equipment (or the “EAR99” designation) prior to its transfer to the excess property office for disposal.

Appendix B

SAMPLE EXPORT CONTROL PROCEDURE SHEET

Export Control Procedures

Date: 13 April 2010

Item Name: Agilent E8361A 10 MHz to 67 GHz PNA Network Analyzer SN- US42370027

Responsible Individual/Title: Issac Newton, Any Group, Acting Group Leader

Organization: Any Lab, Any Division, Any Group

Description: A High Frequency full two-port vector network analyzer. This equipment moves between labs as it is a general use instrument.

Note this equipment is on long term loan to Division 818 from Agilent Technologies as a test bed.
This is NOT GOVERNMENT PROPERTY.

Location(s): Building-Rooms: 24-1003, 24-1300, 24-1400, 24-1500, 1-4608, 1-4078, 1-4080, 1-4632

EAR Controls and Restrictions: Under CCL section 3A002.e, this item is EAR controlled for development and production, but not for use. [NS2, AT1]

Access: Access for use is not restricted, however access is granted to only a limited number of NIST personnel, Foreign Guest Researchers, Affiliates, and visitors. Development and production of this instrument are not carried out at NIST.

Physical Security:

1. Foreign guest researcher, affiliate, and visitor access to this item is monitored by his or her supervisor or sponsor to ensure that it is limited to use only.
2. Rooms 24-1003/1300/1400/1500 are accessible by only selected members of 818.02, the Division Chief and Lab Director. Trilogy locks are in use on all lab doors. The rolling door to the lab is locked or under direct observation when open.
3. Rooms 1-4608/4078/4080 have trilogy locks in use on all doors. Access to the labs will be restricted to authorized personnel when the equipment is in those labs.
4. Room 1-4632 is accessible by only certain members of 818.01, the Division Chief and Lab Director. Trilogy locks are in use on all lab doors.
5. Movement of the devices to from Building 24 will be done only with permission of the 24-1300 Lab Coordinator or their designate and by authorized staff and after signing checkout/EAR acceptance sheet.
6. Access is granted to a limited number of NIST personnel, Foreign Guest Researchers, Affiliates, and visitors. Access codes are not provided to visitors, who must be accompanied at all times. Granting of access codes for room entry is controlled by the Group office, and authorizations are approved by the Group Leader and 818 Division Chief.
7. When not in use or preparation for measurements, the equipment will be turned off and placed behind locked doors.
8. Technical manuals for this instrument are located on the NIST internal file server "Jake" (and can be downloaded from the Agilent website).
9. Contractor and Janitorial staff will not have access to 24-1300 without supervision. NIST maintenance staff will get permission of Lab Coordinator () prior to entrance.

Export Control Procedures (Continued)

10. One cannot learn anything of significance from simply observing the item in operation or by using it.

11. The NIST Physical Security Officer has reviewed and approved these procedures.

Continuity of Service and Operations: The security of this equipment is not impacted by power failure.

Technical: Internal computer control of the instrument is not password protected but it is not connected to the directly to the NIST network. External computer control of the instrument is password protected and is connected to the NIST network. [External control of this item is part of a certified and accredited IT system, and conforms to all IT security requirements established by the NIST CIO.]. Connection via serial (USB/RS-232), local LAN, or IEEE-488 bus will consider the VN A as an allowed peripheral under the NIST IT certification.

Awareness and Training:

1. All operators have been briefed by the Group Leader on the restrictions concerning export controls for this item.
2. All operators receive annual refresher briefings concerning export controls for this item.

Reporting Violations: Individuals who think that export controls have been violated, whether deliberately or by accident, will report their concerns to the Group Leader, who will inform his/her supervisor and the NIST Physical Security Officer.

Approved by the Chief of Emergency
Services Division

Name
Title
Effective Date

Factors for Consideration When Preparing Export Control Procedures

Awareness and Training:

- Who is the one individual responsible for the item (e.g., equipment or software)?
- Is that person aware of any restrictions concerning export?
- Is he or she aware that unauthorized transfer of information may violate export control regulations?
- Who else must have access to the item? (Think beyond the research arena to include janitorial staff, maintenance workers, etc.)
- Are they aware of the restrictions concerning export?
- How are they informed?
- How often are they reminded so that they remain aware?
- What steps should the responsible party or others who may have access to the item take if they feel the regulations have been violated?
- Whom should they consult if they have export compliance questions?

Access:

- Who should not have access to the item?
- How do you prevent their access, but still permit those who must have access to get to the item?

Physical Protection:

- Where is the item (or, in the case of software, access to it) physically located?
How is it secured?
- Where are technical manuals and similar information concerning the item located?
How are they secured?
- Who can see the item? Can someone observing the item in operation, even at a distance, learn anything of significance about it?

Continuity of Service and Operations:

- Is the security of the item impacted by loss of power or any other utility?
(e.g., card access readers don't function if the power is off or the computer system is down)
- If control measures are compromised by a failure or outage, what procedures or fallback controls are in place?

Technical (hardware and software controls that prevent unauthorized access or misuse, and help detect security violations):

- If the item is software, is it on a NIST-approved system?

- Is the mix of physical and logical controls appropriate to preclude inappropriate access, whether deliberate or accidental?

(e.g.; a stand alone computer system that is password protected inside a locked room that only designated NIST employees may enter is extremely well protected. A system that is connected to the NIST network, but has its own internal firewall to preclude inappropriate access, is well protected provided the firewall is frequently updated and the system and its users meet NIST's information security requirements.)

Appendix C

SAMPLE ANNUAL CERTIFICATION

Based on my personal knowledge and the information provided to me by others, I certify the following NIST export control requirements have been completed:

Inventory

The Division/Group/Other Organization (as applicable) has entered into the property accountability (inventory) system the Export Control Classification Number (ECCN) (or “EAR99” designation) for property that is potentially at high-risk for unauthorized inspection, analysis, or use.²

Export Control Procedure Sheets

Export Control Procedure Sheets have been developed for moderate- to high-risk items, updated as needed, and forwarded to the Emergency Services Division.

Foreign National Visitors and Guests

Safeguards are in place within the Division to ensure against the unauthorized release of software and controlled technology to visiting foreign nationals. Division sponsors and escorts have been briefed on export control guidelines and are aware of the steps to take if they feel the guidelines have been violated.

Deemed Exports License List

Software and controlled technology has not been released to foreign nationals in any manner that violates the [Export Administration Regulations \(15 C.F.R. §§ 730–774\)](#). I have attached a list of export licenses that have been obtained or sought (if any) applicable to this certification, indicating to whom and for what the license (or license application) pertains.

Signature_____

Date_____

Name

Title (e.g., Division Chief, Group Leader...)

Completed annual certifications will be maintained on file at Division level for two years.

² Division Chiefs, Group Leaders, and other management and staff as appropriate will work with their property custodians to (a) review and validate the NIST 2010 listing of controlled equipment and enter ECCN information into the property accountability system, and (b) identify high risk or value items not reflected on the 2010 list, or newly acquired, and enter their ECCNs (or “EAR99”) into the property accountability system.

APPENDIX D

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	3/4/2015	Ed Mai (ESD)	First Draft
Rev .01	3/5/2015	Dan Cipra (M&O)	Formatting updates
Rev .02	4/20/2015	Dan Cipra (M&O)	Formatting updates
Rev .03	07/15/2015	Benjamin Overbey	Amended based upon DRB comments document submitted
Rev .04	8/3/2015	Jonathan Hardis (PML)	Memorializing consensus achieved to resolve non-concur votes
Rev. .05	12/15/2015	Dan Cipra	All Comments/changes accepted. Ver 2.

Space Management and Utilization

NIST O 2109.00
Effective Date: 12/3/2015

PURPOSE

This order outlines the requirements and the responsibilities for the management, assignment, and utilization of NIST owned space in order to ensure NIST's compliance with regulatory requirements and federal policies that stress better management practices for efficient utilization of space and the establishment of guidance for the optimization of federal real property. This order should be used in conjunction with NIST PR 2109.01, Space Management and Utilization.

APPLICABILITY

This order applies to all NIST Organizational Units (OUs), as well as occupants of NIST real property from other agencies or organizations, to the extent allowed by law and the terms of the agreements with other agencies or organizations.

LEGAL AUTHORITIES AND REFERENCES

- [NIST Space Board Charter](#), April 18, 2013
- [Executive Order No. 13327](#), *Federal Real Property Asset Management*, February 4, 2004
- [Federal Management Regulation \(FMR\), 41 C.F.R. § 102-79 et seq.](#), *Assignment and Utilization of Space*, January 1, 2011
- [Department Administrative Order \(DAO\) 217-22, Workplace Space Design Standard](#), April 16, 2016
- [Department Administrative Order \(DAO\) 217-21](#), *Space Allowance and Management Program*, August 8, 2013
- [Department of Commerce \(DOC\) Real Property Management Manual](#), August 2014 and subsequent revisions
- [NIST P 2100.00, Facilities and Site Management Policy](#), August 28, 2015

REQUIREMENTS

- Develop, implement, and administer a practical space management and utilization program;
- Assign space equitably among OU's, taking into consideration their staffing and program requirements;

- Ensure effective and economical use of NIST owned space as guided by the legal authorities and reference documents listed above;
- Comply with Department of Commerce (DOC) space utilization goals for Office and Office Support Space;
- Maintain an accurate record of all space owned and managed by NIST with regard to occupancy and usage for the purposes of responding to inquiries from DOC and achieving departmental goals;
- Complete annual real property reporting to DOC.

DEFINITIONS

NIST Space Database – The official record of all NIST-owned space maintained to comply with regulatory requirements.

Occupant Type – A field in the NIST Database denoted as either: full-time permanent (FTP), part-time/cyclical (PTC), non-agency full-time (NAF), or non-agency part-time (NAP).

Real Property – Fixed (unmovable) property, principally land and buildings, and also rights and interests with respect to this property (NIST P 2100.00 Facilities and Site Management).

Reserve Space – Space not assigned to any OU/Chief Office and categorized as Reserve Space in the NIST Space Database.

Space Board – A standing committee comprised of the Chief Facilities Management Officer, Associate Director for Management Resources, Associate Director for Laboratory Programs, Associate Director for Innovation and Industry Services, NIST Chief of Staff, and the Boulder Laboratories Director with oversight authority regarding space use and assignments on all NIST sites.

Space Utilization per Person – A measure of the average USF occupied per person for Office and Office Support space types (Space Types 1.00 – 1.06 in the NIST Space Database).

Usable Square Feet - The actual area the agency occupies in an office suite. It is the office area, workstation area, conference rooms, kitchenettes, server closets, storage rooms, and circulation within the office suite area.

RESPONSIBILITIES AND AUTHORITIES

NIST Director

- Complies with all regulatory requirements.

Space Board:

- Exercises authority over space use and assignments on all NIST sites;
- Formulates and institutes NIST space management-related policies, procedures and requirements, incorporating policy direction from DOC; and
- Evaluate Space Requests and establish priorities for space assignments

- Make decisions for the assignment of space to individuals NIST OUs
- Approve the reassignment of OU-vacated space to the NIST Reserve

Associate Director for Management Resources

- Certifies the annual Federal Real Property Profile report to DOC;
- Chief Facilities Management Officer
- Serves on the NIST Space Board Committee as Chair;
- Advises the Space Board on changing federal policies affecting this order; and

Space Program Analyst, Office of Facilities and Property Management (OFPM)

- Drafts revisions to the order and procedures.
- Manages all NIST-owned space for compliance with federal and departmental regulations, policies and guidelines;
- Maintains the NIST Space Database;
- Provides OU users with access to the NIST Space Database;
- Conducts space utilization analyses;
- Prepares the annual Federal Real Property Profile report to DOC using NIST Space Database;
- Reviews the requesting OU's existing space for areas that may be underutilized;
- Identifies possible solutions that more efficiently use a requesting OU's existing space; and
- Communicates with all affected OU's regarding proposed space request solutions.

OU Directors

- Ensure that necessary actions are taken to effectively manage the space allocated to their OU;
- Review and approve requests for additional space for their OU using the Space Request Form NIST-261; and
- Ensure that space is returned to the NIST Reserve when conditions under Reserve Space are met (as stated in NIST PR 2109.01, Space Management and Utilization Procedure).

OU Senior Management Analysts or Executive Officers

- Manage the space allocated to their OU to resolve space needs internally as much as possible;
- Process requests for additional space for their OU using the Space Request Form NIST-261;

- Contact the Space Program Analyst, OFPM to return space to the NIST Reserve when conditions under Reserve Space are met;
- Complete the NIST-1221 for all occupant relocations to ensure space data is updated in the NIST Space Database; and
- Update and verify the accuracy of their OU's data in the NIST Space Database.

DIRECTIVE OWNER

190 - Chief Facilities Management Officer

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Rev. 1.01	12/3/2015	Dan Cipra	Published Ver. 1
Rev. 1.02	07/28/2016	Amber Hayes	Incorporated OCC interim comments and legal guidance.

Space Management and Utilization Procedure

NIST PR 2109.01
Effective Date: 12/3/2015

PURPOSE

This procedure is for the management, assignment, and utilization of NIST owned space and should be used in conjunction with NIST O 2109.00, Space Management and Utilization.

APPLICABILITY

This procedure applies to all NIST Organizational Units (OUs), as well as occupants of NIST real property from other agencies or organizations, to the extent allowed by law and the terms of the agreements or licenses with other agencies or organizations.

LEGAL AUTHORITIES AND REFERENCES

- [NIST Space Board Charter](#) 4/18/2013
- [Space Request Form, NIST-261](#)
- [Telecommunications Service Request and Directory Information, NIST-1221](#)
- NIST O 2109.00 Space Management and Utilization (12/03/2015)
- DAO 217-21 DOC, Space Allowance and Management Program (2013-08-08)

SPACE ALLOCATION PROCESS

Organizational Unit (OU) Directors manage the space allocated to their OU and ensure that necessary actions are taken to effectively use that space. To the fullest extent possible, the OU Directors solve their space needs internally.

New Space Request

When a request for additional space is necessary, the following space request process occurs:

- a. The OU Senior Management Advisor (SMA) shall complete the Space Request Form (NIST Form 261), which requires approval from the OU's Director, and submit it to the Space Program Analyst, Office of Facilities and Property Management (OFPM). A request for additional space should include an explanation of why the requested space could not be found within the OU's existing space and a description of the need and programmatic justification for additional space, in addition to the specifications for requested space. The OU SMA must comply with the Department of Commerce (DOC) established goal of less than or equal to 170 net assignable square feet (USF) (15.8 sq.

meters) per person on average for Office and Office Support space types (See Appendix B for a list).

- b. The Space Program Analyst reviews the requesting OU's existing space for areas that may be underutilized. When possible, the Space Program Analyst will make suggestions to more efficiently use the OU's existing space, and to accommodate the additional space requested.
- c. The Space Program Analyst calculates the space utilization rate for the requesting OU. If >170 USF (15.8 sq. meters) per person on average for Office and Office Support space, the OU is asked to look within their existing space. The Space Program Analyst can provide advice to maximize space utilization. If <170 USF (15.8 sq. meters) per person on average for Office and Office Support space, the Space Program Analyst will look for additional space, typically from reserves or a neighboring OU's space. Notification will be provided to the affected OU Division(s) at the time proposed solutions are identified, and communications with the affected OU Division(s) will take place prior to finalizing a space change decision.
- d. The Space Program Analyst presents a proposed solution to the requesting OU, considering various factors such as: safety and security considerations, location and adjacency requirements, modifications that would be required, availability of the space and the urgency of the space need. All requests, with recommended solutions, will be presented to the Space Board for decisions to be made in the best interest of NIST overall.
- e. Approved space reassignments are documented in a memorandum, which are used to inform the requesting OU and the NIST Director, and to create a record for the Space Board and Space Program Analyst.
- f. If the Space Board is unable to come to a consensus, the NIST Director shall make a final decision.

Space Transfers Between OUs

- a. Proposed transfers of allocated space between OUs are submitted to the Space Program Analyst. Required information, including building, room number, changes in occupancy, occupant name, occupant type [e.g., full-time permanent (FTP), part-time/cyclical (PTC), non-agency full-time (NAF), or non-agency part-time (NAP)], and room use shall be provided.
- b. The Space Program Analyst will present proposed space transfers to the NIST Space Board for approval/concurrence.
- c. The approved space transfer is documented by the Space Program Analyst in a Space Change Memorandum.
- d. The Space Program Analyst will update the NIST Space Database (See Appendix A for list of field names) accordingly.

Reserve Space

- a. When organizational changes result in space moves within or between OUs, the Space Program Analyst, OFPM will conduct an analysis of the remaining space utilization, to ensure efficient use of the space and to determine whether there is a need to reallocate any space to Reserve.
- b. Space must be returned to the NIST Reserve under the following conditions:
 - 1) When space is vacated due to a relocation from the NIST site, where staff is presently located.
 - 2) When space is vacated due to an elimination or reduction of program or staff.
 - 3) When a program is moved to a newly constructed or renovated building.
- c. The NIST-261 should be used to return space to Reserve.
- d. Space should be returned to Reserve in an acceptable condition. Laboratories should be decommissioned and declared hazard-free by the NIST Office of Safety, Health & Environment.

Temporary Assignments

The Office of Facilities and Property Management and the NIST Space Board may assign space on a temporary basis. Temporary assignments are documented in a memorandum and reviewed periodically.

Space Management System

The NIST Space Database is updated:

- with the results of the annual NIST Space Survey,
- when organizational changes occur, and
- when space allocations or transfers are authorized.

Staffing information is updated by OUs and automatically populated nightly from the Central People Repository, which is a central human resources data repository. All staff moves must be processed using the NIST-1221 to ensure accurate data in the Central People Repository and the NIST Space Database.

Space Utilization Review

- a. OU Directors shall ensure that space within their OU is continuously reviewed for full and efficient use of their space.
- b. The Space Program Analyst performs Space Surveys of all NIST sites annually. Detailed reports by building and organization are supplied to each OU/Chief Office. Each OU's SMA completes the reports by providing all necessary revisions/updates, and returns the data to the Space Program Analyst, who enters changes into the NIST Space Database to reflect the new data.

- c. The Space Program Analyst performs walk-through inspections of assigned space throughout the year to verify the space records and review the utilization.

DIRECTIVE OWNER

190 - Chief Facilities Management Officer

APPENDICES

- A. NIST Space Database Information Fields
- B. Space Type Classifications
- C. Space Change Memo Template
- D. Revision History

APPENDIX A

NIST Space Database Information Fields

Organizational Unit/Division and Assigned Group - Identifies the Group number assigned to the space (Code 990 is the NIST Reserve and Code 999 is used to identify Reserve space that has been assigned but not taken over by the new Group).

Bldg. - Identifies building assignment by number (e.g., Metrology is entered as 220).

Room - Identifies the room number. The building number and the room number uniquely identify a space.

Room Description - Describes what the space is being used for. Please be as descriptive as possible. If the space has more than one use or more than one group is using it, please indicate and note the square footage for each use/user.

NIST Code - Identifies space usage by categories used by NIST. These categories are narrower than those used by GSA/DOC.

Commerce Code - Identifies space usage by categories established by GSA.

Sq. Ft. - The net square footage of a room. If a room has more than one Group using it or more than one type of use, the square footage should be divided accordingly.

Occupant - Identifies the user/occupant of the room. All persons using a space should be listed.

Employee Group - This indicates the Group number of the occupant (e.g., 161.01 for the Formulation and Financial Management Group of the Budget Division).

Employee Type:

FTP - Identifies full-time permanent space occupants and should be filled in with a "1" if the occupant is full time permanent. This should only be shown once for each person, preferably next to the person's office space. It should not be filled in each time a person is listed.

PTC - Identifies part-time, temporary or cyclical positions and should be filled in with a "1" if the occupant is part-time, temporary, or cyclical. This should only be shown once, preferably next to the person's office space.

NAF - Identifies non-agency, full-time individuals and should be filled in with a "1" if the occupant works in NIST space greater than 39 hours per week for 52 weeks per year, and does not appear on the personnel roster as a NIST employee.

NAP - Identifies non-agency part-time individuals and should be filled in with a "1" if the occupant works in NIST space at least one month out of the year, and does not appear on the personnel roster as a NIST employee.

APPENDIX B

Space-Type Classifications

NIST Code	NIST Space Types	NIST Description	Corresponding DOC Space Types
01.00	OFFICE	Typical office environment with desks & computers. Basic power & environmental control requirements. No laboratory-type infrastructure services.	OFFICE
01.01	PRIVATE CONFERENCE	Conference or meeting space proximate to office space & assigned to an Organizational Unit/Chief Office.	OFFICE
01.02	COPY/MAIL/FAX	A work room typically at a Division or OU/Chief Office level to serve personnel on one of more levels.	OFFICE
01.03	FILES or STORAGE	A central repository space for all OU/Chief Office/Division files & storage of office supplies, publications, etc.	OFFICE
01.04	BREAK-ROOM	An employee break-area that may include some space for eating. Typical appliances include a microwave & a refrigerator. Plumbing or a sink is normally available.	OFFICE
01.05	PRIVATE LIBRARY	A library within an OU/Chief Office/Division space housing reference & research materials unique to the organization.	OFFICE
01.06	TRAINING/ CLASSROOM	Space designated for teaching purposes & equipped with projection screen/smart board or other teaching tools. Space may support computer network & audio-visual equipment.	OFFICE
02.00	STORAGE (Only DIV. 192 & Bldg. 203)	Central storage that houses supplies & equipment for all OUs. Infrastructure requires no plumbing & minimal power. The space may not be finished.	WAREHOUSE
02.01	OTHER STORAGE	Storage space assigned to specific OUs for their exclusive use.	GENERAL STORAGE
02.02	LAB STORAGE	Storage space assigned to specific OUs for their exclusive use for laboratory storage.	LAB STORAGE
03.00	CONFERENCE (Only Div. 107)	Conference table & chairs. Generally has audio/visual screen, black boards, etc.	CONFERENCE/ TRAINING
04.11	GPL - DRY LAB	Probably has no hood, has minimum plumbing, okay to have sink & drain.	LABORATORIES /CLINIC
04.12	GPL - WET LAB	Has wet hood(s), one or several of - vacuum, gas, hot & cold water, drain, sinks, (i.e. - heavy plumbing).	LABORATORIES /CLINIC
04.13	GPL - CLEAN ROOM	HEPA filtered, laminar flow hoods, wall treatments, infiltration control, generally high air volumes, probably has special walls & suspended ceiling.	LABORATORIES /CLINIC
04.14	COMPUTER	Computer intensive workstations for the purpose of	LABORATORIES

	LAB	research. May require additional power & environment control but does not require any of the general laboratory infrastructures.	/CLINIC
04.21	HIGH BAY	Above 14 ft. ceiling, generally convenient access to grade, dry, probably has crane or hoists.	LABORATORIES /CLINIC
04.23	HIGH BAY SPECIAL	Above 14 ft. ceiling, wet/dry, designed for specific use such as, nuclear reactor, environmental chamber, or electromagnetic shielding, probably has crane or hoist.	LABORATORIES /CLINIC
04.24	LOW BAY SPECIAL	Ceiling height less than 14 ft., wet/dry, designed for special use.	LABORATORIES /CLINIC
05.00	LIBRARIES	Designated book storage & research area.	STRUCTURALLY CHANGED
06.00	EXHIBITS	Designated exhibit & museum area.	STRUCTURALLY CHANGED
08.00	CONCESSIONS	Food preparation, sales & eating area. Can include areas designated for vending machines.	FOOD SERVICES
09.00	AUDITORIUM S	Has stage area & row seating.	STRUCTURALLY CHANGED
10.00	RESTROOM/ LOCKER	Ceramic tile on floors & walls, exhaust fans, & toilet room fixtures.	
11.00	FACILITY SUPPORT	Mechanical, electrical, & elevator rooms.	LIGHT INDUSTRIAL
11.01	OCCUPIABLE FACILITY SUPPORT	Space is used for support of NIST but provides a suitable environment in its present state for an office operation.	LIGHT INDUSTRIAL
11.02	SERVICE GALLEY	Utility corridor or Lab support corridor.	LIGHT INDUSTRIAL
11.03	FACILITY SUPPORT (Non- Mechanical)	Space is used to support NIST, and in its present state, can only be used for this purpose. Includes Plant Division space, such as, the Shops.	LIGHT INDUSTRIAL
12.00	ADP	Computer rooms. Generally has raised floor & computer room air conditioning units.	ADP

APPENDIX C

SPACE CHANGE MEMO TEMPLATE

MEMORANDUM FOR (name)
Director, (OU)

From: (name)
Chief Facilities Management Officer

Subject: OU Space Usage
(Temporary Space or Permanent Space Use in Building ###)

The following space usage was approved on (date):

The following space may be (temporarily/permanent) used by: (OU).

Building	Room	From Div	To Div	Space Type	Sq. Ft. (Assignable)	Comments
###	###	###	###	#.##	###	(Temporary)

Effective Date: (date)

Background/Description:
(Background description gathered from Space Request Form.)

Space Decision:
(Description of approval/disapproval and temporary/permanent assignment.)

Approved:

(name), CFMO
Chair, NIST Space Board

Date

cc: (ADMR)
(ADIIS)
(ADLP)
(NIST Chief of Staff)
(Planning and Space Management Team Leader)
(Planning and Space Management Space Analyst)
(OU SMA)

bc: (CFMO)
(Locksmith)
Space File

APPENDIX D

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Rev 1.01	12/3/2015	Dan Cipra (M&O)	Original Published Version 1
Rev 1.02	7/28/2016	Amber Hayes	Incorporated OCC interim comments and legal guidance.

Emergency Management

NIST P 2200.00

Effective Date: 8/20/2012

PURPOSE

Direct the establishment of an effective and efficient emergency management framework for transitioning from normal operations to a coordinated NIST emergency response across a wide range of emergencies.

SCOPE

This policy applies to all sites owned and operated by NIST and to all NIST employees, associates and visitors at such sites.

LEGAL AUTHORITY AND REFERENCES

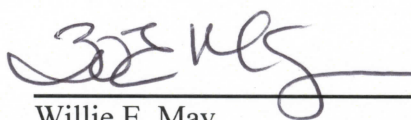
- [The NIST Act, 15 United States Code §§ 271 et seq.](#)
- Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*.
- [Homeland Security Presidential Directive #5, Management of Domestic Incidents](#).
- [Homeland Security Presidential Directive #8, National Preparedness](#).
- [Emergency Readiness for Department Continuity, Department Administrative Order \(DAO\) 210-1](#).
- [Commerce Responsibilities in Disasters, DAO 210-7](#).

POLICY

It shall be the policy of NIST to establish a comprehensive, effective and efficient agency-wide approach to emergency management to ensure the safety, protection and security of NIST employees, associates, visitors and infrastructure across a broad spectrum of emergencies.

NIST's emergency management approach shall address preparedness, protection, response and recovery, and provide for a seamless continuity of operations through a single, comprehensive organizational structure for the management of emergency responses to natural, man-made and terrorist events. The NIST approach shall be consistent with applicable Executive Orders, other directives, and with the National Response Framework. NIST shall coordinate and integrate its emergency management efforts with those of local, State and Federal entities, as appropriate.

The Associate Director for Management Resources shall ensure the development of other directives as necessary for the full and effective implementation of this policy.



Willie E. May
Director

7/24/15

Date

Emergency Management Program

NIST O 2201.00
Effective Date: 11/5/2014

PURPOSE

This directive establishes requirements, responsibilities, and authorities for the development, implementation, and oversight for the National Institute for Standards and Technology's (NIST) Emergency Management Program through the application of the NIST Emergency Management Organization and Incident Management Concept of Operations strategy at NIST-administered sites. The strategy identifies roles and responsibilities and authorizes the issuance of related guidance for implementation. This directive provides the framework for the transition from normal operations to a coordinated emergency response in support of all hazards at NIST-administered sites.

APPLICABILITY

This directive applies to all NIST employees and associates whether or not they are actively engaged in the incident response. Site occupants shall obey all instructions provided by the Emergency Management Organization.

This directive applies to NIST-administered sites in Maryland, Colorado and Hawaii.

REFERENCES

This directive complies with and implements applicable Executive Orders, Homeland Security Presidential Directives, statutes, interagency directives, Department Administrative Orders (DAOs), Department of Commerce (DOC) regulations, and NIST guidance involving safety, security, and threat management, including but not limited to:

- [The Homeland Security Act of 2002](#), (as amended) an Act to establish the Department of Homeland Security whose primary mission includes preparedness of the United States for acts of terrorism.
- [Executive Order \(E.O.\) 12656](#), Assignment of Emergency Preparedness Responsibilities
- [Executive Order \(E.O.\) 12472](#), Assignment of National Security and Emergency Preparedness Telecommunications Functions
- [Presidential Policy Directive #8 \(PPD-8\)](#), National Preparedness
- [Presidential Decision Directive \(PDD\) 63](#), Critical Infrastructure Protection
- [Presidential Decision Directive \(PDD\) 67](#), Enduring Constitutional Government and Continuity of Government Operations (classified)
- [Homeland Security Presidential Directive #5 \(HSPD-5\)](#), Management of Domestic Incidents

- [Homeland Security Presidential Directive #7 \(HSPD-7\)](#), Critical Infrastructure Identification, Prioritization, and Protection
- [Homeland Security Presidential Directive #8 \(HSPD-8\)](#), National Preparedness
- [The National Response Framework](#)
- [Federal Continuity Directive 1 \(FCD 1\)](#), Federal Executive Branch National Continuity Program and Requirements
- [Federal Continuity Directive 2 \(FCD 2\)](#), Federal Executive Branch Mission Essential Functions and Primary Mission Essential Function Identification and Submission Process
- [Department Administrative Order \(DAO\) 210-1](#), Emergency Readiness for Departmental Continuity
- [Department Administrative Order \(DAO\) 210-7](#), Commerce Responsibilities in Disasters, Department of Commerce Manual of Security, Policy and Procedures

BACKGROUND

The goal is to execute NIST's emergency management responsibilities:

- to support the National Response Framework (NRF) concepts, processes, and structures;
- to support the national preparedness program;
- to support all hazards incident response;
- to support agency Continuity of Operations Plan (COOP) functions and responsibilities; and,
- to assure the safety, protection, and security of federal employees, associates, contractors and visitors, and infrastructure on NIST-administered sites.

The Emergency Management Organization is comprised of the following elements:

- the Emergency Management Planning and Support Team which assists the Emergency Services Office (ESO) in the development and implementation of the program;
- the Incident Management Team composed of the Senior Leadership Team and the Emergency Operations Team that supports the on-scene Incident Commander; and
- the Evacuation Coordinator Team that assists NIST ESO and OSHE in the protection of personnel in an all hazards incident.

The Incident Management Concept of Operations (IM CONOPS) establishes a comprehensive, agency-wide approach to incident management across the spectrum of incident activities and functions to include: prevention, preparedness, protection, response, recovery and mitigation. NIST's incident management CONOPS integrates agency activities and assures balanced and coordinated integration into local and national plans along with organizational structures. The CONOPS ensures NIST's approach is consistent, flexible, resilient and adaptable. NIST's IM CONOPS:

- provides a common organizational framework;

- facilitates seamless coordination;
- implements use of a common lexicon for effective communications; and
- optimizes situational awareness to build a common operating picture shared by all engaged NIST elements: those impacted by the incident, those deployed on-site, and those operating at normal duty stations.

NIST has specific responsibilities identified within the National Response Framework for the delivery and application of Federal resources and capabilities to support a response to an incident. This includes the following Emergency Support Functions (ESF):

- ESF #3 Public Works and Engineering: Providing technical support and advice on the procurement of external consulting services for assessing structural and fire safety of damaged buildings and lifelines (public works and utilities);
- ESF #7 Logistics Management and Resource Support: Providing technical expertise on structural surveys as well as the procurement of external consulting services to assess structural and fire safety of Federal and non-Federal damaged buildings and lifelines;
- ESF #14 Community Recovery: Providing building science expertise (i.e., National Construction Safety Team for deployment after events causing the failure of a building resulting in a significant loss of life).

DEFINITIONS

Agency – A permanent or semi-permanent organization within the Federal Government that is responsible for the oversight and administration of specific functions. Within the context of this order, NIST is an agency that is subordinate to the Department of Commerce. The NIST Boulder Laboratories facility hosts elements of two additional agencies: the National Oceanic and Atmospheric Administration (NOAA) and the National Telecommunications and Information Administration (NTIA). NIST, NOAA and NTIA are also referred to as bureaus of the Department of Commerce.

All Hazards Incident – An all hazards incident is an incident that needs an organized response by a public, private, and/or governmental entity to protect life, public health and safety, values to be protected, and to minimize any disruption of governmental, social, and economic services. The all hazards incident may be natural or human-caused. An all hazards incident response may include multiple responses (search, rescue, evacuation) to one or more kinds of incidents (fire, flood, mass casualty) occurring simultaneously.

Common Operational Picture (COP) – A single identical display of relevant operational information shared by more than one command. A COP facilitates collaborative planning and assists incident responders in achieving situational awareness.

Continuity of Operations Plan (COOP) – United States Federal initiative, required by Presidential directive, to ensure that agencies are able to continue performance of essential functions under a broad range of circumstances.

Designated Official (DO) – The official to whom is delegated the assigned responsibility for activating site or facility emergency plans.

Emergency Management Senior Leadership Team (SLT) – One of two components of the Incident Management Team, one element of the Emergency Management Organization on a site. The SLT is removed from the EOC and composed of executives; it provides an executive level view of Situational Awareness.

Emergency Management Organization (EMO) – The group of teams responsible for the emergency management program for the Site and for the Operating Units on the site.

Emergency Operations Center (EOC) – A central command and control facility responsible for carrying out the principles of emergency preparedness and emergency management, or disaster management functions at a strategic level in an emergency situation, and ensuring the continuity of operation of a company, political subdivision or other organization.

Emergency Operations Center (EOC) Manager – The one individual in charge of the EOC.

Emergency Operations Plans – The plans for managing a wide variety of potential hazards.

Emergency Operations Team (EOT) – The team of people working in the EOC under the direction of the EOC Manager.

Emergency Response Providers – Federal, state, and local government public safety, law enforcement and other emergency responders, emergency medical and related personnel, agencies, facilities, and/or authorities designated to respond in emergency situations.

First Responder – Local and nongovernmental police, fire and emergency personnel who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence and the environment.

Incident – An occurrence or event, natural or human-caused, which requires an emergency response to protect life or property.

Incident Commander – The individual responsible for all incident activities, including the development of strategies and tactics and ordering and releasing resources.

Incident Command System (ICS) – A systematic tool used for the command, control, and coordination of emergency response; a subcomponent of the National Incident Management System (NIMS).

Incident Command System Structure – The hierarchical system established by ICS.

Mission Essential Functions (MEFs) – The limited set of department-and agency-level government functions that must be continued throughout or resumed rapidly after a disruption of normal activities.

National Incident Management System (NIMS) – A system mandated by HSPD-5 that provides a consistent, nationwide approach to domestic incident response, regardless of cause, size or complexity.

National Response Framework (NRF) – Part of the National Strategy for Homeland Security that presents the guiding principles enabling all levels of domestic response partners to prepare for and provide a unified national response to disasters and emergencies. Building on the existing (NIMS) as well as (ICS) standardization, the NRF's coordinating structures are always in effect for implementation at any level and at any time for local, state, and national emergency or disaster response.

NIST Emergency Program Manager – The individual who develops NIST directives and procedures and establishes the standards for compliance of the program at NIST-administered sites.

Occupant Emergency Plan (OEP) – A set of procedures to protect life and property in federally occupied space under defined emergency conditions.

Organizational Units (OUs) – The subordinate NIST organizations on the site delineated by mission focus.

Shelter in Place (SIP) – An emergency action in which facility occupants are sheltered in a protected location within the facility in lieu of evacuation. Situations in which SIP may be appropriate include civil unrest, certain weather emergencies, atmospheric release of toxic substances and other external hazards.

Site – Contiguous geographic location of NIST assets under NIST administrative control. NIST has sites in Gaithersburg Maryland, Boulder and Fort Collins Colorado, and Kauai, Hawaii.

Site Emergency Program Manager – The individual who develops implementing instructions and local plans for NIST sites to establish a NIMS compliant emergency management program.

Site Incident Response Organization – The element of the EMO which may be activated to respond to an incident on the site.

Site Manager – The individual designated by the NIST Director for the Safety, Security and Emergency Management on a NIST-administered site.

Site occupants – A term utilized to include employees, associates, affiliates, contractors and visitors to NIST-administered sites.

Situational Awareness – The ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission. More simply, it's knowing what is going on around you.

Situation Report (SITREP) – Recurring report that records and describes a particular incident and the response.

REQUIREMENTS AND PRINCIPLES

NIST must establish a comprehensive, agency-wide approach to incident management across the spectrum of incident activities and functions to include: prevention, preparedness, protection, response, recovery and mitigation.

The site Emergency Management Organizations (EMOs), in executing these incident management responsibilities, shall ensure a consistent, flexible, resilient and an adaptable approach which assures balanced and coordinated integration into local and national emergency plans along with organizational structures.

Incident management's goal is to reduce human risk resulting from natural or human-induced emergencies and to ensure capabilities are fully integrated into emergency planning and available at all times. This is achieved through:

1. Protecting life (highest priority), property, and the environment.
2. Meeting the immediate emergency needs of the situation.
3. Mitigating hazards that pose a threat to life, property, and the environment.
4. Restoring essential functions, facilities and supporting activities that are essential to NIST's mission.

NIST will achieve this by:

- Developing and maintaining emergency management plans and procedures.
- Maintaining liaison with appropriate Federal, State and local authorities (DOC Emergency Operations Center (EOC); Federal, State and Local EOC's; etc.).
- Designating an Emergency Management Organization (EMO).
- Developing, maintaining and updating the OEP.
- Developing tabletops, training, testing and exercising scenarios to assure the viability of plans currently in place and to update as necessary.
- Providing assistance to non-NIST entities as prescribed by law, Executive Order, Department Administrative Order, or whenever possible upon:
 - Request from other federal agencies for emergency assistance and support.
 - Request from local governments that have declared a Local Emergency.
 - Direction from the Department of Homeland Security to render emergency assistance.
 - Gubernatorial Declaration (Maryland or Colorado) of a state of emergency.
 - A Federal declaration of a state of war or national emergency.

RESPONSIBILITIES AND AUTHORITIES

NIST Director / Under Secretary of Commerce for Standards and Technology (Under Secretary)

- Responsible for the overall incident management prevention, preparedness, response, recovery and mitigation at NIST-administered sites.
- Ensures NIST's ability to meet mission requirements through contingency planning, training personnel, and executing remedial actions identified during drills and exercises.
- Delegates the authority to execute the responsibilities contained herein through the Associate Director for Management Resources.

NIST Associate Director for Management Resources (ADMR)

- Ensures NIST's ability to meet mission requirements through contingency planning, training personnel, and executing remedial actions identified during drills and exercises.
- Provides strategic guidance and direction on the NIST emergency management program.
- Chairs the Senior Management Team for COOP and the EOC.
- Functions as the Designated Official for Gaithersburg.
- Establishes the Emergency Management Program through the promulgation of plans and procedures.
- Oversees the Emergency Services Office Chief in the execution of this Program.

Chief of the Emergency Services Office (ESO)

- Serves as the NIST Director's advisor on issues relating to emergency management programs.
- Responsible for All Hazards Incident Management.
- Develops and maintains the NIST Emergency Management directives and all supplemental guidance ensuring NIST compliance with the aforementioned references.
- Provides programmatic emergency management guidance and oversight to NIST-administered sites.

Organizational Unit (OU) Directors:

- Responsible for the development and implementation of OU-specific emergency plans and programs.
- Ensures all staff are aware of emergency management procedures and comply with instructions during an incident.

Site Occupants:

- Shall read the [Occupant Emergency Plan \(OEP\)](#) and comply with its contents.
- Are responsible for the safety of their visitors and the visitor's compliance with emergency procedures during an incident.

Designated Official (DO) / Site Manager

Gaithersburg Site	Boulder Site
Associate Director for Management Resources	Boulder Laboratories Site Manager

- Provides guidance and direction to the Site Emergency Program Manager.
- Ensures Incident Management Team's ability to meet mission requirements hereunder.
- Oversees the establishment of working relationships with state and federal agencies that might respond to an emergency in the facility.
- Oversees the implementation of the Emergency Management Program on the site.
- Member of the Emergency Management Planning and Support Team.
- Responsible for the development of the OEP.

Site Emergency Program Manager

Gaithersburg Site	Boulder Site
Emergency Services Office Chief	NIST Emergency Management Program Manager

- Ensures all Emergency Management Program directives and guidance adhere to the all hazards policies and protocols in accordance with NIST emergency management procedures, National Response Framework (NRF) and other FEMA guidance.
- Coordinates and directs site efforts to prevent, protect, respond, recover, and mitigate all hazards (with or without COOP activation).
- Manages the NIST Emergency Operations Center (EOC).
- Issues training, exercises, and all supplemental emergency management guidance.
- Oversees the conduct of orientation and training for EOC participants.
- Acts as the site liaison with the Department of Commerce Office of Security and other Federal agencies.
- Develops and implements site operational policies and procedures to supplement this Directive.

Emergency Management Organization (EMO)

The EMO is responsible for:

- Assisting the ESO in the development and implementation of the program;

- Supporting the EOC and Incident Commander during emergency incidents and/or COOP activations; and
- Assisting ESO and OSHE in the protection of personnel in all hazards incidents.

DIRECTIVE OWNER

137 – Emergency Services Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Draft	10/5/2016	Ed Mai	Updated for new office ESD to ESO
Rev. 2.0	10/12/2016	Dan Cipra	Made all changes per DO

Energy Contingencies Procedure

NIST PR 2201.03
Effective Date: 3/21/2016

PURPOSE

This procedure details responsibilities and prescribes procedures for adjusting to energy shortages in accordance with [10 Code of Federal Regulations 436.105](#), for the safety of personnel and buildings, and for the continuity of critical experiments and processes during shortages of electrical power, natural gas/heating oil, and/or motor vehicle fuel.

APPLICABILITY

This procedure applies to the two main NIST sites, Gaithersburg, MD and Boulder, CO, and does not apply to the two radio stations, Fort Collins, CO and Kauai, HI.

REFERENCES

- [10 Code of Federal Regulations \(CFR\) 436.105](#) Emergency Conservation Plan
- [O 2201.00 Emergency Management Program](#) (11/5/2014)
- [O 2107.00 Energy and Sustainability Management Program](#) (2/4/2016)

BACKGROUND

As required by the Department of Energy's Emergency Conservation Plan ([10 CFR 436.105](#)) for Federal agencies, NIST shall:

- i) Maintain plans, including priorities, for temporarily reducing missions, services, and other activities, to assuage the impact of a sudden disruption in the supply of electrical power, natural gas, or oil-based fuels;
- ii) Provide for the testing of emergency actions to ascertain their effectiveness; and
- iii) Implement the appropriate plan to deal with and adjust to local shortages in energy supply.

DEFINITIONS

Designated Officials

The Chief Facilities Management Officer (CFMO) or his/ her designee is the Designated Officials (DO) responsible for decision making and reporting for NIST with regard to energy contingency planning.

Designated Energy Contingency Coordinators

The following are the Designated Energy Contingency Coordinators (DECCs):

- i) Chief, Boulder Maintenance and Support Services Division, for electricity and natural gas/heating oil for the Boulder, Fort Collins, and Kauai sites;
- ii) Chief, Gaithersburg Facility Maintenance Division, for electricity and natural gas/heating oil for the Gaithersburg site; and
- iii) Chief, Facilities Services Division, for motor vehicle fuel on the Gaithersburg, Boulder, Fort Collins, and Kauai sites.

Critical Experiments and Processes

For this Procedure, experiments and processes are either “Critical” or “Interruptible”. Critical experiments and processes are those that cannot be interrupted because the interruption will result in more than one day’s loss of data results and/or personnel will be unduly or unusually exposed to hazardous or unsafe conditions.

Interruptible Experiments and Processes

Interruptible experiments and processes are those that can be paused with no more than one day's loss of results and/or with no undue or unusual exposure of personnel to hazardous or unsafe conditions.

Key Division Personnel

Key personnel within the three Office of Facilities and Property Management (OFPM) divisions (Boulder Maintenance and Support Services, Facilities Maintenance, and Facilities Services), as designated by their respective Division Chiefs, are to be notified by the DECCs and to serve as active liaisons during emergency outages and/or planned utility interruptions.

RESPONSIBILITIES

Designated Energy Contingency Coordinators:

- Obtain and maintain Department of Energy guidance on energy emergency planning;
- Develop and maintain general energy contingency plans for the various sites and obtain appropriate official approval for these plans;
- Develop and maintain detailed contingency plans for electrical power and natural gas for individual buildings and coordinate these plans with the occupants; and
- Implement the contingency plans in consultation with the DOs.

NIST Division Chiefs (and acting Division Chiefs):

- Develop and maintain a list of critical experiments and processes and equipment that should receive priority attention during a shortage of electrical power or natural gas. It should be noted that Organizational Units (OUs) are responsible for the programmatic

costs associated with ensuring emergency backup power is available to the experiments and processes they deem as critical during a shortage of electricity or natural gas.

- Annually on February 1 or as priorities shift, provide an updated copy of their list of critical experiments and processes and/or equipment to:
 - a) Chief, Boulder Maintenance and Support Services Division for systems located in Boulder; and to
 - b) Chief, Gaithersburg Facility Maintenance Division for systems in Gaithersburg.
- Ensure the safety of their division personnel and operations during contingencies.

Key Division Personnel:

- Notify appropriate employees in their division (as designated by their Division Chief) of energy contingency and outage events. If a division member cannot be reached, key division personnel shall leave a message for the “uncontacted” person and report the absence to their Division Chief.
- Maintain an active liaison during contingencies and outages with the Boulder Maintenance and Support Services Division or the Gaithersburg Facility Maintenance Division, depending upon their location.

ENERGY CONTINGENCY PLANS

1. Plans for each site shall include provisions for:
 - i) Reacting to the specified energy shortage;
 - (1) Appendix A describes the plan for electrical power
 - (2) Appendix B describes the plan for natural gas / heating oil
 - (3) Appendix C describes the plan for motor vehicle fuel
 - ii) Informing personnel and maintaining proper communications;
 - iii) Maintaining critical experiments, processes, activities, and/or equipment; and
 - iv) Protecting personnel and facilities.
2. The DECCs at each site shall give copies of the energy contingency plans to their key division personnel and other staff members who may be directly involved in contingency actions and shall make other distribution of the plans as appropriate.
3. A separate plan provides direction for two Energy Contingency Planning Events:
 - i) Energy Emergency: This is when energy contingency plans are actually implemented due to an actual loss or imminent loss of power.
 - ii) Energy Alert: An alert shall typically result from an email or telephone call from an energy supplier indicating an actual or imminent reduction in supply. It might also be

a declaration of an emergency by the President. At this point, a decision needs to be made by the respective DECC as to the extent of the energy contingency plan to be recommended for implementation to the NIST Director.

COMMUNICATIONS

1. For energy emergencies requiring immediate notification and evacuation, the NIST Emergency Notification System (ENS) will be used to notify NIST staff of the need to implement the Energy Contingency Plan. For energy emergencies that are recognized at least two hours in advance, as well as energy contingencies such as “brown outs” and “curtailment of services”, the DECCs shall use site-wide emails and GovDelivery notices to inform the NIST staff.

i) Energy emergency notification using ENS –

(1) Boulder: Initial notification that evacuation or early dismissal is necessary is received from the NIST Director or another official source. The BLSM shall notify the Boulder Laboratories Director, the Director of NTIA, and the Executive Director for NOAA Labs. The BLSM shall prepare the message that activates the ENS for Boulder.

(2) Gaithersburg: Initial notification that evacuation or early dismissal is necessary is received from the NIST Director or another official source. The CFMO shall direct the Emergency Coordinator to prepare the message that activates the ENS for the Gaithersburg site.

ii) Energy Alert – Energy alerts may arrive in two ways:

(1) If the DECC receives an alert, s/he shall inform the CFMO who in turn shall inform the NIST Director and the BLSM.

(2) If the CFMO receives an alert directly, the CFMO’s office shall notify the NIST Director and the BLSM. Depending on the type and location of the shortage, the CFMO shall also inform the Boulder Maintenance and Support Services Division Chief or the Gaithersburg Facility Maintenance Division Chief for shortages of electricity and/or natural gas, or the Facility Services Division Chief for shortages of motor vehicle fuel.

The DECCs shall determine whether to notify all NIST staff or to pass along information only to the affected OUs and their key division personnel.

2. For the purpose of transmitting utility outage information, a list of OU and Chief Office’s key personnel shall be maintained by the Boulder Maintenance and Support Services Division and the Gaithersburg Facility Maintenance Division. This information shall be provided to the DECCs by the NIST Divisions Chiefs in their annual February 1 update of critical experiments and processes and/or equipment.

3. When the energy contingency ends and there is a call to “return to normal”, a notice shall be communicated in the same manner that the event was originally announced.

DIRECTIVE OWNER

190 – Deputy Director Office of Facilities and Property Management

APPENDICES

- A. Electrical Power
- B. Natural Gas/Heating Oil
- C. Motor Vehicle Fuel
- D. Revision History

APPENDIX A

ELECTRICAL POWER

This electrical energy contingency plan applies to contingencies which may arise as a result of requests by Xcel Energy of Colorado or Pepco Energy Service of Maryland or the Department of Commerce to reduce electrical energy consumption. This plan does not cover the contingency which would result from an instantaneous complete loss of electricity. All actions described below shall be given maximum priority consistent with safe operating procedures.

ACTIONS

To conserve electricity during a shortage:

- * Lights, experiments, processes, and air-conditioning unit (ACU) fans shall be safely switched off in the order shown below, to the extent believed necessary.
- * Lights in offices and laboratories shall be switched off by the occupants.
- * Lights in other areas and ACU fans shall be switched off at Boulder by the Maintenance and Support Services Division and at Gaithersburg by the Facility Maintenance Division.
- * Interruptible experiments and processes shall be shut down by the responsible research staff.

When ACU fans are turned off, room temperatures shall heat up at a rate dependent upon their interior and exterior heat loads.

SHUTDOWN SEQUENCE
a. For Gaithersburg – implement Plant Division Instruction 2.13, Chilled Water Load Shedding Plan in conjunction with Energy Conservation Measure 14.1 protocol. Temporarily lower the supply discharge temperature of the site’s chilled water loop before an event and then raise the loop’s discharge temperature during the event sufficiently so that the demand for chilled water is reduced and one of the large chillers can be secured.
b. Shut off lights in aboveground exterior wall modules, stairwells with windows, cafeterias, and other areas where the lights are not needed.
c. Shut down non-critical perimeter and office ACU fans.
d. Shut down all interruptible experiments and processes using electricity. When hoods are involved, researchers shall secure experiment work inside the hood and lower the sash to a safe minimum height. (Interruptible experiments and processes are those which can be paused with no more than one day's loss of results and/or with no undue or unusual exposure of personnel to hazardous or unsafe conditions.)

e. Shut down all remaining perimeter and office ACUs for several hours per night and on weekends. For this step, key OU division personnel shall be asked at Boulder by the Maintenance and Support Services Division and at Gaithersburg by the Facility Maintenance Division to identify all exhaust hoods that can be shut down 24 hours per day to help maintain air balance and to limit the amount of already conditioned air being exhausted.

f. Shut down all remaining ACUs that serve interruptible experiments and processes for several hours per night and on weekends.

g. Obtain additional reductions by selecting one or more of the following options (the choice shall depend upon the circumstances):

- (1) Match Central Plant's chilled water generating capacity with the reduced load.
- (2) Consider shutting off ACU units noted in b., d., and e. above for 24 hours per day.
- (3) Operate emergency generator at Building 225 (that supplies power to the Central Computing Facility) to partially offset electric commercial grid power supplied to this building (in Gaithersburg only).
- (4) Evaluate with the researchers in Buildings 230 and 245 A-Wing if wind tunnel (230) and horizontal air flow simulator (245) operations can be secured during the energy contingency period. (in Gaithersburg only)
- (5) Evaluate with the NCNR management as to what operations can be secured during the energy contingency period. (in Gaithersburg only)

h. Shut down all remaining ACUs and exhaust hoods, including those for experiments and processes on the critical list.

APPENDIX B

NATURAL GAS/HEATING OIL

This energy contingency plan applies to contingencies which may arise as a result of a shortage of natural gas or heating oil. Conservation efforts shall help reduce the impact of shortages and decrease the chances of critical experiments and processes being shut down. Electricity shall not be affected by a natural gas/heating oil shortage and lights should not be turned off. All actions described below shall be given maximum priority consistent with safe operating procedures.

ACTIONS

To conserve natural gas/heating oil during a shortage, air discharge temperatures for HVAC units that serve admin spaces and space temperature set shall be lowered and exhaust hoods shall be safely switched off in the order shown below, to the extent believed necessary. This plan does not cover the contingency which would result from a complete loss of natural gas/heating oil.

SHUTDOWN SEQUENCE

a. For Gaithersburg – the boilers at the Central Plant have dual fuel capability. If there is a shortage of natural gas, switch the necessary number of Central Plant boilers' fuel supply to heating oil. -The Combined Heat and Power Plant is not dual fuel capable; accordingly, its operation would be secured.

For Boulder – Boulder Maintenance and Support Services Division (BMSS) will lower the thermostats in buildings to reduce consumption and scale back on the humidity control in the PML.

b. Shut off non-critical perimeter and office ACU units which are not already being switched off for several hours per night and on weekends as a normal energy conservation measure. Ensure freeze-stat protection is functional on these units. In Gaithersburg only – shut off humidity pots.

c. Shut off all remaining perimeter and office units for several hours per night and on weekends. Ensure freeze-stat protection is functional on these units. For this step, key OU division personnel in Boulder and Gaithersburg shall identify exhaust hoods that can be shut down 24 hours per day to help maintain air balance and to limit the amount of already conditioned air being exhausted. In Gaithersburg only – shut off humidity pots.

d. Shut off all remaining ACUs that serve interruptible experiments and processes for several hours per night and on weekends. Ensure freeze-stat protection is functional on these units. In Gaithersburg only – shut off humidity pots.

e. Shut off any additional exhaust hoods identified by key OU personnel as being non-critical.

f. Set temperature for laboratory interruptible experiment spaces to 65 °F or as is appropriate.

g. Shut off all ACU units in b., c., and d. above, from several hours per day to 24 hours per day.

h. Shut off all remaining units (ACUs and exhaust hoods), including those for experiments and processes on the critical list. Set building reheat system to protect buildings.

APPENDIX C

MOTOR VEHICLE FUEL

This energy contingency plan applies to contingencies which may arise as a result of a shortage of motor vehicle fuel (diesel and gasoline). Conservation efforts shall help reduce the impact of any shortages.

ACTIONS

To achieve the planned reductions, diesel and gasoline shall be rationed as follows:

- a) Physical security and fire protection services shall be maintained at their current level of fuel usage, but this allocation may be altered by the Facilities Services Division (FSD) as circumstances warrant and after discussion with the Chief, Emergency Services Division.
- b) Fuel shall be rationed to the remaining activities in the following priority to achieve the required reduction in NIST fuel usage.
 - 1) Operating Units with uninterruptible research needs, and only to the degree necessary to support those uninterruptible requirements.
 - 2) Facility Maintenance Division, as necessary to maintain the minimum level of transport response vehicles for corrective, critical maintenance.
 - 3) Facility Services Division, only as necessary to support uninterruptible research operations
 - 4) Shuttle services for off-campus pickup and delivery.
- c) Available fuel levels will be determined by FSD, based on the fuel usage experienced during the most recent twelve-month period for which data is available and on the amount of fuel expected to be available to NIST, based on the emergency conditions creating the contingency. Within each OU and Chief Office, rationing shall be prorated as directed by the OU Director or Chief Officer. FSD shall implement the rationing by issuing expected fuel allocations via email to the Organizational Units. OU Heads should anticipate potential changes to these values based on actual emergency conditions. These allocations shall not be affected, either positively or negatively, by unused values from a prior month, although changing conditions of the emergency may alter allocation levels.

Note - Physical security is the only portion of this Appendix C plan that applies to Boulder, Fort Collins, and Kauai. These three sites do not have their own fire protection services or a shuttle service. Fuel is also not provided to divisions other than Boulder's Maintenance and Support Services Division and the Design and Construction Division.

APPENDIX D

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	1/20/2016	John Bollinger	Initial Draft
Rev. 1	1/20/2016	Dan Cipra	Formatting Updates
Rev. 2	1/24/2016	John Bollinger	Addressed comments from Dan Cipra
Rev. 3	3/9/2016	John Bollinger	Addressed DRB review comments
Rev. 4			

Smoking Policy

NIST P 2300.00

Effective Date: **APR 04 2016**

PURPOSE

To establish a smoking Policy for NIST in accordance with Executive Order 13058, entitled "*Protecting Federal Employees and the Public from Exposure to Tobacco Smoke in the Federal Workplace.*"

SCOPE

This Policy is applicable to all NIST employees, associates, and visitors, to the extent allowed by law and the terms of the Associate's agreement on sites owned and operated by NIST.

LEGAL AUTHORITY

- [Executive Order No. 13058, 62 Fed. Reg. 43451 \(Aug. 9, 1997\)](#) "Protecting Federal Employees and the Public from Exposure to Tobacco Smoke in the Federal Workplace"

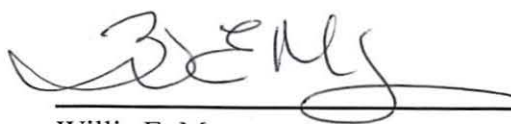
POLICY

It is NIST Policy to protect non-smoking employees, associates, and visitors on sites owned and operated by NIST from exposure to environmental tobacco smoke from cigarettes, cigars, pipes, and other sources.

This Policy will be implemented by establishing designated smoking areas in outdoor locations away from air intake ducts, building entrances, walkways, parking lots, and other areas where non-smoking employees, associates, and visitors could be exposed to environmental tobacco smoke. The efficacy of the implementation of the Policy will be reviewed within five years of its issuance to determine if additional actions are necessary to protect employees, associates, and visitors.

NIST encourages and supports employees who request assistance in eliminating dependence on the use of tobacco products.

The Associate Director for Management Resources (ADMR) shall ensure the development of other directives necessary for the full and effective implementation of this Policy.



Willie E. May
Director

APR 04 2016

Date

Security

NIST P 2400.00
Effective Date: 10/21/2016

PURPOSE

To establish the National Institute of Standards and Technology (NIST) policy for ensuring the security of NIST personnel, buildings and other plant facilities, equipment, property and assets.

SCOPE

This policy applies to all NIST employees and associates, to the extent allowed by law and the terms of the associate's agreement.

LEGAL AUTHORITY

- [15 United States Code § 278e\(b\)](#).
- [The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard](#), August 2013
- [Department of Commerce \(DoC\) Organization Order 20-6](#), Director for Security
- [DoC Organization Order 30-2A](#), National Institute of Standards and Technology
- [DoC Security Manual of Policies and Procedures](#), Office of Security, December 2012

POLICY

It is NIST's policy to establish and maintain a comprehensive, effective and efficient agency-wide approach to ensuring the security of NIST personnel, buildings and other plant facilities, equipment, property and assets, while maintaining a world-class laboratory-based research and development organization. NIST is committed to accomplishing this, and to safeguarding the NIST mission, by:

- Systematically identifying and mitigating security risks.
- Integrating security considerations systematically into operations at all levels, including all aspects of work planning and execution.
- Providing the resources and support necessary for employees and associates to conduct their work in a secure environment.
- Engaging employees and associates in the execution of security measures, along with security preparedness education and training programs.

- Fostering an environment in which employees and associates are encouraged to report and raise security concerns without fear of retaliation.
- Continually improving the effectiveness and efficiency of NIST's security processes, systems, and capabilities through assessments, performance benchmarks, and cost metrics.
- Ensuring the NIST security program evolves and adjusts to emerging threats.
- Ensuring compliance with applicable laws, Executive Orders, regulations, and directives.
- Setting and communicating clear and sustainable security objectives.
- Balancing the need to preserve an atmosphere conducive to research and collaboration while achieving a secure environment at NIST.

In addition, every individual to which this directive applies is expected to:

- Take responsibility for their own security and the security of their co-workers and guests.
- Be alert and mindful of security at all times.
- Immediately report any security concerns to, and cooperate with, appropriate security personnel.
- Display U.S. Government-issued ID at all times when on a NIST campus, or in a NIST building or facility.
- Participate in security preparedness education and training opportunities.
- Remind coworkers and visitors of security procedures or practices at NIST.
- Ensure that others are displaying their U.S. Government-issued ID while on a NIST campus or in a NIST building or facility.
- Correct deficiencies and take actions to prevent security incidents from occurring.
- Promptly report security incidents.
- Share security information and lessons learned.

The Associate Director for Management Resources shall ensure the development of other directives necessary for the full and effective implementation of this policy.



Willie E. May
Director

10/21/16
Date

Facility Access Cards and Electronic Access Control

NIST PR 2401.01

Effective Date: 6/8/2016

PURPOSE

This directive establishes responsibilities and procedures for the issuance, display, replacement and relinquishment of National Institute of Standards and Technology's (NIST) Facility Access Cards (herein referred to as the NIST FAC), and includes: Personal Identification Verification (PIV), site, facility user, visitor, and limited access cards and the design, implementation, and maintenance of enterprise-wide access control systems for the safeguarding of people and assets applicable to all NIST-owned and operated sites. This directive identifies roles and responsibilities and authorizes the issuance of related guidance for implementation.

APPLICABILITY

This directive is applicable to all NIST-owned and operated sites. Electronic access affects NIST employees and Associates located at those sites to the extent allowed by law and the terms of the Associate's Agreement.

REFERENCES

- [41 CFR 101.20.103](#), Physical Protection and Building Security.
- [41 CFR 101.20.3](#), Conduct on Federal Property.
- Department of Commerce, [Security Manual of Policies and Procedures](#), Office of Security, December 2012.
- Department of Commerce, [Department Administrative Orders \(DAO\) 207-12, Foreign National Visitor and Guest Access Program](#).
- [Risk Management Process for Federal Facilities: An Interagency Security Committee Standard](#), Department of Homeland Security, August 2013.
- [Homeland Security Presidential Directive 12 \(HSPD-12\)](#), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
- [OMB M-11-11](#), Continued Implementation of HSPD-12 Policy for Common Identification Standard for Federal Employees and Contractors, February 3, 2011.
- [P 2100.00](#), Facilities and Site Management Policy.
- [P 1400.00](#), Visiting Research and Associate Policy.

- [O 1401.00](#), Domestic Associates Program.
- [O 1402.00](#), Foreign Guest Researcher Program.
- [N 6103.09](#), Access and Use of Personal Identity Verification (PIV) Card Authentication to Information Systems.
- [Real ID Act, Department of Homeland Security, December 20, 2013.](#)

DEFINITIONS

Access Control System (ACS) – software/hardware solution that controls access to specific facilities.

Access Requirement Document (ARD) – A Department of Commerce (DOC) form developed for processing of Foreign Nationals (FN) in accordance with the Department Administrative Order (DAO) 207-12.

Activation – a process whereby the card recipient places the PIV card in the PIV card reader and is prompted for a password (PIN) and the card is “personalized” with the recipient’s security certificates.

Associate/Affiliate – an individual who works at NIST sites but is not employed by NIST. Refer to the [NAIS Associate types](#) for description of each. (Boulder utilizes the term affiliate to mean associate.)

Badge – card bearing information, as one's name, logo or place of employment, or academic affiliation, for visual identification purposes (see also NIST FAC).

Badge Office – the central point where cards are issued to employees and non-NIST employees.

Certificate – is an electronic digital signature installed on the PIV card chip to bind a public key with an identity – information such as the name of a person or an organization, their address, etc.

Color Codes for Cards – blue stripe: foreign national associate; green stripe: domestic associate; and yellow card: limited access, no color stripe for employees.

Common Access Cards (CAC) - a type of "Smart" ID card for active-duty military personnel, Selected Reserve, Department of Defense civilian employees, and eligible contractor personnel.

Electronic access control – controlling entry into a physical area by means of a controller and electronic components including: locks, readers, sensors, buttons and more. Electronic access control specifies who can go where and when.

Employee – a full-time or part-time Federal employee of the National Institute of Standards and Technology.

Enrollment – process whereby the applicant enrolls in the USAccess system for a PIV credential, presents the proper identification documents, has photo and fingerprints captured and verifies personal information provided.

Facility User Card – card issued to NIST Center for Neutron Research (NCNR) users. CNST facility users are issued a Site Card.

Foreign National (FN) – any person who is not a citizen or legal permanent resident of the United States of America.

Guest – see [DAO 207-12](#) for definition and must be registered in the Visitor Registration System and entered into NAIS.

Guest Researcher – a type of associate who collaborates with NIST on research projects of mutual interest, and/or works under a federal funding agreement with a U.S. university or U.S. company. (see [Associate/Affiliate](#) definition and [NAIS Associate types](#).)

Human Resource Arrivals and Departure System (HRADS) – system that controls the status of employees.

Intergovernmental Personnel Act (IPA) – Authorizes assignments made to or from federal agencies and the following: state and local governments; private and public colleges and universities; Indian Tribal governments; federally-funded research and development centers; and qualified non-profit organizations involved in public management. Assignments must be with the consent of the employee and for work of mutual benefit to the organizations involved.

Limited Access PCard – Yellow identification card with visual image issued to kiss & ride, child care center and visitors' applicants (construction, maintenance, service providers, delivery personnel, etc.) and does not permit electronic access authority at NIST sites.

NIST Associate Information System (NAIS) – Automated system that supports the process of bringing NIST associates, affiliates, contractors, guest researches, other federal employees, and all non-NIST individuals to the NIST campus or allowing access to NIST resources.

NIST Facility Access Card (FAC) – overall name provided for a visually identifiable card that represents the various card types issued by the NIST Badge Office.

Personal Identification Number (PIN) - a secret string of numbers that a claimant memorizes and uses to authenticate his or her identity. PINs are generally 6-8 digits.

Personal Identification Verification (PIV) Card – a physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Physical Access Control System (PACS) – software/hardware solution system that controls access to facilities on the NIST campus. [Also see Access Control System (ACS).]

Piggybacking – when another person follows through a door with permission of the person who has access to a restricted area.

Police Services Group (PSG) – Federal police officers responsible for physical protection of the site, traffic enforcement, motor vehicle and crime investigations, and emergency response.

Protective Security Officer (PSO) – contract security guard that operates security posts at NIST access/egress gates.

Security-hours – also referred to as out-of-hours, after-business hours or after hours. The period from 7:00 pm to 6:00 am Monday through Friday and all hours Saturday, Sunday and holidays.

Site Card – NIST-issued temporary card valid for less than 179 days, cumulatively in a calendar year, that permits electronic access authority to NIST sites. For PIV-required individuals the site card will only be valid for 45 days.

Sponsor, Department Sponsor (DS) or NAIS Host – a U.S. citizen and NIST Federal employee responsible for the day-to-day activities associated with the visitor/guest during their duration at NIST administered sites.

Tailgating – when another person passes through a restricted door without the knowledge of the person who has gained legitimate access to a restricted area.

Vehicle Registration – State-issued official document that contains vehicle, owner, tag information, proof of insurance, and proof of ownership (the title) of the car.

White Visitor Card – A card issued to an individual who is only visiting the site for a limited duration and is sponsored by an employee of NIST and does not permit electronic access authority at NIST sites. All visitors must be escorted by their sponsor while on the site.

Visitor – see DAO 207-12 for definition, individuals must be registered in the Visitor Registration System.

Visitor Registration System – A NIST web-based system where departmental sponsors enter information on visitors to the campus.

FORMS

[CD-591](#) - *Department of Commerce Personal Identity Verification (PIV) Request*

[DAO 207-12 Attachment 2](#) - *Certification of Conditions and Responsibilities for Departmental Sponsors or Foreign National Guests*

[DAO 207-12 Attachment 3](#) - *Certification of Conditions and Responsibilities for Foreign National Guest*

[DN-42](#) - *Report of Loss/Theft of NIST Identification Badge*, form used to notify proper authorities for lost, damaged, or stolen NIST FAC.

[DN-52](#) – *Limited Access Pass Application Authorization for Release of Information* to be completed and submitted to the Badge Office for processing and approval.

[NIST-351](#) – *Request for Federal Credential or NIST Site Badge [NIST Federal Employee]*, a NIST electronic form used to request a PIV or NIST-Issued Site Card.

[NIST-1260](#) – *Report of Foreign Visitor(s), Guest(s), Conference Attendee(s)*, a NIST electronic form used to report Foreign Visitor(s), Guest(s), and Conference Attendee(s).

[NIST-1284](#) – *Access Change Request*, an electronic form used to request an access change.

DELEGATION OF AUTHORITY

The NIST Director hereby delegates the Director of the Office of Facilities and Property Management (OFPM) authority to provide management of the HSPD-12 program.

The Director of OFPM hereby delegates to the Chief, Emergency Services Division, oversight of the badging program.

RESPONSIBILITIES FOR BADGING

NIST Director

- Has overall responsibility for compliance with HSPD-12 and other applicable federal regulations regarding badging of employees, associates, etc.

Organizational Unit (OU) Directors

- Ensure that new employees and eligible Associates/Affiliates apply for and receive a NIST FAC.
- Process special requests for modified access authorizations for NIST employees and non-NIST employees.
- Ensure all PIV card holders comply with the Office of Information Systems Management (OISM) [logical access policy](#).

Office of Human Resources Management (OHRM)

- Ensure each new eligible employee is entered into HRADS and the USAccess system for a PIV card.
- Ensure the correct designation and card type is assigned to PIV card as applicable, i.e., Emergency Response Official (ERO).
- Ensure that new Federal employees proceed to the Badge Office for a photograph and receipt of their Site card until their PIV card is received.
- Inform Federal employees to bring two (2) forms of identification for enrollment in the USAccess system.
- Terminate the employee status in USAccess system when Federal employees leave or transfer from the agency.

Department Sponsors (DS)

- Ensure NAIS Initiators enter correct information into the NAIS system for sponsored [domestic](#) or [foreign national](#) Associates/Affiliates.
- Attend counterintelligence briefings provided by the NIST Office of Security (OSY) annually for sponsoring of FNs.
- Review roles/responsibilities with sponsored Associates/Affiliates while on NIST administered sites.
- Review and sign the [DAO 207-12 Attachment 2](#), for each foreign national for each agreement period, Certification of Conditions and Responsibilities for Departmental Sponsors or Foreign National Guests.
- Review the [DAO 207-12 Attachment 3](#), for each foreign national for each agreement period, ensure the Foreign National Guests understands the restriction for their appointment. Ensure that the [DAO 207-12 Attachment 3](#) is signed by the FN associate/affiliate and provided to OSY through NAIS.
- Submit an [Access Requirement Document](#) (ARD) in accordance with Department of Commerce DAO 207-12 Foreign Guest Access to NIST OSY.
- Ensure the USAccess sponsor, for their organization, terminate the PIV card in the USAccess system when the individual leaves NIST.
 - Collect the PIV card / site card issued and return to the Badge Office.
 - Ensure NAIS is updated when Associate/Affiliate departs and sends notification to OSY and the Emergency Services Division (ESD) through NAIS.

NIST Office of Security (OSY)

- Conduct background investigations and provide decisions to Badge Office for issuance of cards.
- Approve/disapprove (NIST-1260) foreign visit requests to NIST-owned and operated sites and promptly notify DS and ESD of the decision.
- Provide counterintelligence briefings annually and upon request to NIST employees.
- Approve/disapprove requests for access during security-hours to Associates/Affiliates/Contractors and FNs and promptly notify DS and ESD of the decision.
- Notify OHRM, DS, ESD, and Contracting Officer Representative (COR) when an individual's card request has been denied.

International and Academic Affairs Office (IAAO)

- Process foreign national Associates/Affiliates who meet the requirements for a PIV card into the General Services Administration (GSA) USAccess system.

- Direct foreign national Associates/Affiliates to OSY for processing.

Technology Partnerships Office (TPO)

- Process NIST Associates/Affiliates who meet the requirements for a PIV card into the USAccess system.
- Direct Associates/Affiliates to the Badge Office for processing.

NIST Center for Neutron Research (NCNR)

- Process/create cards for employees and Associates/Affiliates requiring special access as Facility Users to Building 235.
- Process employees and Associates/Affiliates into the NCNR ACS.

Badge Office

- For PIV enrollment – capture fingerprints and photographs, validate two (2) forms of identification provided, and enroll the individual into the USAccess system.
- Issue appropriate card type for employees and Associates/Affiliates and enter information into the PACS.
- Notify and send reminders to individuals that their PIV card is available for pickup and assist in the activation of the credential.
- Import PIV card into the PACS.
- Assign appropriate access levels
- Assist individuals, as needed, with updating their PIV card certificates.
- Process requests for renewal and reissue cards.
- Act as sponsor for individuals not previously entered into USAccess system (Gaithersburg).
- Update site / PIV cards with additional access levels as authorized and inform the individual / DS of the change.
- Import CAC into access control system (Boulder).
- Issue PIN for Child Care Center (CCC) parents/guardians and Conference attendees (Boulder).
- Issue parking permit (exception: handicap and vanpool are issued by DOC PSG).

Visitor Center (VC)

- Issue White Visitor Card to registered visitors.
- Distribute NCNR access cards, created/delivered to the VC by the NCNR User Office, to NCNR Facility Users.

- Provide directions and guidance to visitors new to the NIST site.
- Process and capture fingerprints for submission to the respective OSY security office per agency procedures (Boulder only)

Employees and Associates/Affiliates/Contractors

- Ensure the NIST FAC is physically displayed at all times while on NIST campus and follow the rules of behavior as specified within this procedure.
- Within the timeline provided in the notice complete enrollments, activations, certificate updates, and renewal requests of their PIV card when notified.
- Within 48 hours report the loss, damage, or theft of their NIST FAC to their supervisor and the Badge Office. Complete forms NIST-351 for OHRM and DN-42 for submission to ESD.
- Report damaged or non-functioning NIST FAC to the Badge Office.
- Ensure correct information is entered into the Visitor Registration System for visitors/guests to the NIST campus.
- Upon receipt of their PIV card, individuals must utilize it to gain access to NIST facilities and must comply with OISM's [logical access policy](#).
- Except where authorized by ESD, individuals must surrender their Site card upon receipt of their PIV card.
- Upon separation or departure from NIST, individuals must return their issued NIST FAC to the Badge Office.

Protective Security Officers

- Main gate – issue temporary White Visitor Card during security-hours.
- Distribute NCNR access cards, as necessary, to users during security-hours (Gaithersburg).
- Distributes Child Care Center, Vendor, Contractor, Family Spouse, and Conference Badges (Boulder).

BADGING PROCEDURES (see Appendix A for diagram)

Initial Entry for All Individuals to the Campus

1. All individuals must first report to the NIST Visitor Center before entering site.
2. Visitor Center verifies that the individual has been entered into the Visitor Registration System for access.
3. Visitor Center receives email or faxed form for NOAA/NTIA requesting access.(Boulder)

4. Individuals must provide one (1) form of identification ([Real ID Act](#)) and a vehicle registration document if operating a motor vehicle (Gaithersburg).
5. Visitor Center staff validates information and provides a White Visitor Card and a temporary parking pass to the individual. Staff directs individuals to appropriate location.
6. New employees, Associates/Affiliates/contractors will be required to have a background check prior to issuance of a NIST FAC.
7. TPO processes domestic Associates/Affiliates while IAAO processes FN and legal permanent resident Associates/Affiliates, then individuals proceed to OSY.
8. OSY approves/disapproves requests for NIST FAC, and submits information to NAIS and directs the individual to the Badge Office to receive his or her NIST FAC (Gaithersburg only).
9. OSY approves/disapproves requests for NIST FAC, and informs the DS Associates/Affiliates is approved for access and can proceed to Badge Office for processing (Boulder).
10. NCNR Facility Users proceed directly to NCNR to be processed for a Facility User's card. CNST Facility Users will be directed to CNST NanoFab User Office and will be escorted to the Badge Office to receive a Site Card.

Site Card Procedures for Associates/Affiliates/Contractors (all Non-NIST employees)

1. DS ensures all Associate/Affiliate/Contractors (all non-NIST employees) are entered into the NAIS system for access to NIST administered sites.
2. All applicants will be required to have a (E-QIP) background check prior to issuance of a card.
3. NIST OSY approves application and enters the information into NAIS.
4. Badge Office verifies information in NAIS for Associates/Affiliates.

For those individuals who do not require a PIV card, the Badge Office provides the individual with a Site Card for the duration of their agreement. For those requiring a PIV Card, the Badge Office will provide the individual with a Site Card valid for 45 days. Individuals requiring IT access for any duration will receive a PIV Card.

PIV Procedures for Employees/Associates

1. All applicants will be required to have a background check prior to issuance of a card.
2. A Site Card will be issued for temporary physical access pending issuance of a PIV card or for individuals who are not eligible to receive a PIV card.
3. Upon notification of sponsorship into the USAccess system, individual schedules an enrollment appointment, and reports to Badge Office with two (2) forms of identification.

4. Badge Office validates documents against USAccess record, captures fingerprints and photograph of individual.
5. Upon receipt of e-mail notification of PIV card for pickup, individuals will immediately schedule an appointment in accordance with the instructions in the e-mail. Failure to do so may result in a lapse in physical access to the NIST campus.
6. Badge Office will assist the individual with the activation of the PIV card and PIN requirements.
7. Upon receipt of e-mail notification to update the digital certificate on the PIV card, the individual must immediately schedule an appointment in accordance with the instructions in the e-mail. Failure to do so will result in a lapse of logical access.
8. Badge Office will assist the individual with the certificate update process of the PIV card.
9. Badge Office and iTAC will assist individuals who require PIN resets.
10. Sponsors requesting security-hours access for Associates/Affiliates must provide NIST-1284 for approval through NAIS (Gaithersburg). Boulder must submit the NIST-1284 for OSY approval of security-hours access via NAIS and the [site-access request form](#).
11. Sponsors of FNs must follow NIST directives [O1402.00](#) and [PR1402.01](#).
12. Upon receipt of e-mail notification for a renewal credential for pickup, individual immediately schedules an appointment in accordance with the instructions in the e-mail.

Card Procedures for Limited Access Card

1. All individuals must be sponsored by a NIST employee, who must complete and submit a DN-52.
 - Foreign Nationals must be approved for access by the Office of Security.
 - Chief, Facilities Services Division (FSD) sponsors/approves non-affiliated child care center applicants.
2. All applicants will be required to have a criminal background check prior to issuance of a Limited Access Card.
3. Once the application has been approved, the sponsor is notified via e-mail.
 - The sponsor must register the applicant in the Visitor Registration System for the applicant to be issued a White Visitor Card at the Visitor Center.
 - The sponsor will escort the visitor to the Badge Office to be issued the card. The applicant must present two (2) forms of identification prior to issuance.
4. Vendors and/or service providers who have been authorized for unescorted building access may pick up a one-day vendor/service card issued by ESD, Building 318 (Gaithersburg). Applicant will be required to provide driver's license at that time and upon completion of the service/delivery, return the one-day card to the Police Services Group.

Specific badging procedures for the National Oceanic and Atmospheric Administration (NOAA), the National Telecommunications and Information Administration (NTIA) and GSA in Boulder are found in Appendix C.

RESPONSIBILITIES FOR ACCESS CONTROL

NIST Director

- Ensures logical and physical access control measures are in place for the overall security of NIST sites.
- Delegates to the Chief, ESD oversight of the electronic access control program.
- Ensures compliance with Commerce Acquisition Manual (CAM) chapter on [Personnel Security Requirements](#) as it relates to contractors accessing NIST networks and facilities.
- Expects all occupants of NIST-owned and operated sites to comply with this directive.

Organizational Units/Divisions/Offices

- Submit all requests for new access control points or modifications to the existing system to ESD for review and approval.
- Report all unauthorized access or compromised cards/pins immediately to the ESD.
- Provide a list of authorized users by lock/facility locations to the ESD. All changes and modifications to this authorized user list must be reported to the ESD within two days of implementation.
- Only authorizes the access necessary to meet mission requirements and such access must be consistent with the individual's NIST site access (days and times).
- Set the PACS and/or ACS PIN anti-tamper lockout to 3 invalid attempts.
- Bear the cost for the implementation of new access control points or modifications to the PACS and/or ACS system.

Emergency Services Division (ESD)

- Designs, implements and manages all access control systems for NIST (NCNR & NANO-Fab ACS excluded), including but not limited to:
 - The management, maintenance and expansion of the physical access control system (PACS);
 - Approving of all ACS for use at NIST;
 - Reviewing of all requests for access control devices and installation plans;
 - Defining procedures and practices to be used where ACS are to be utilized;
 - Identifying ESD personnel who must be granted access in all ACS implementations;
- and,

- Developing criteria for the submission of both types of request for access control devices (stand-alone and NIST-wide).
- Approves all access controls systems utilized at NIST.
- Only authorizes the use of a PIN of 8 characters in length if the individual does not yet possess a PIV card. Once an individual receives his or her PIV Card, it must be programmed into each access control point and given the appropriate access (Boulder).

All FAC holders

- Based on the limitations of the ACS, individuals must ensure controlled doors are properly secured at all times (they cannot be propped open) and must not permit any “piggybacking/tailgating” entry of others. Escorted visitors/guests must remain with the Department Sponsor (DS) during their visit.

DIRECTIVE OWNER

190 – Office of Facilities and Property Management (OFPM)

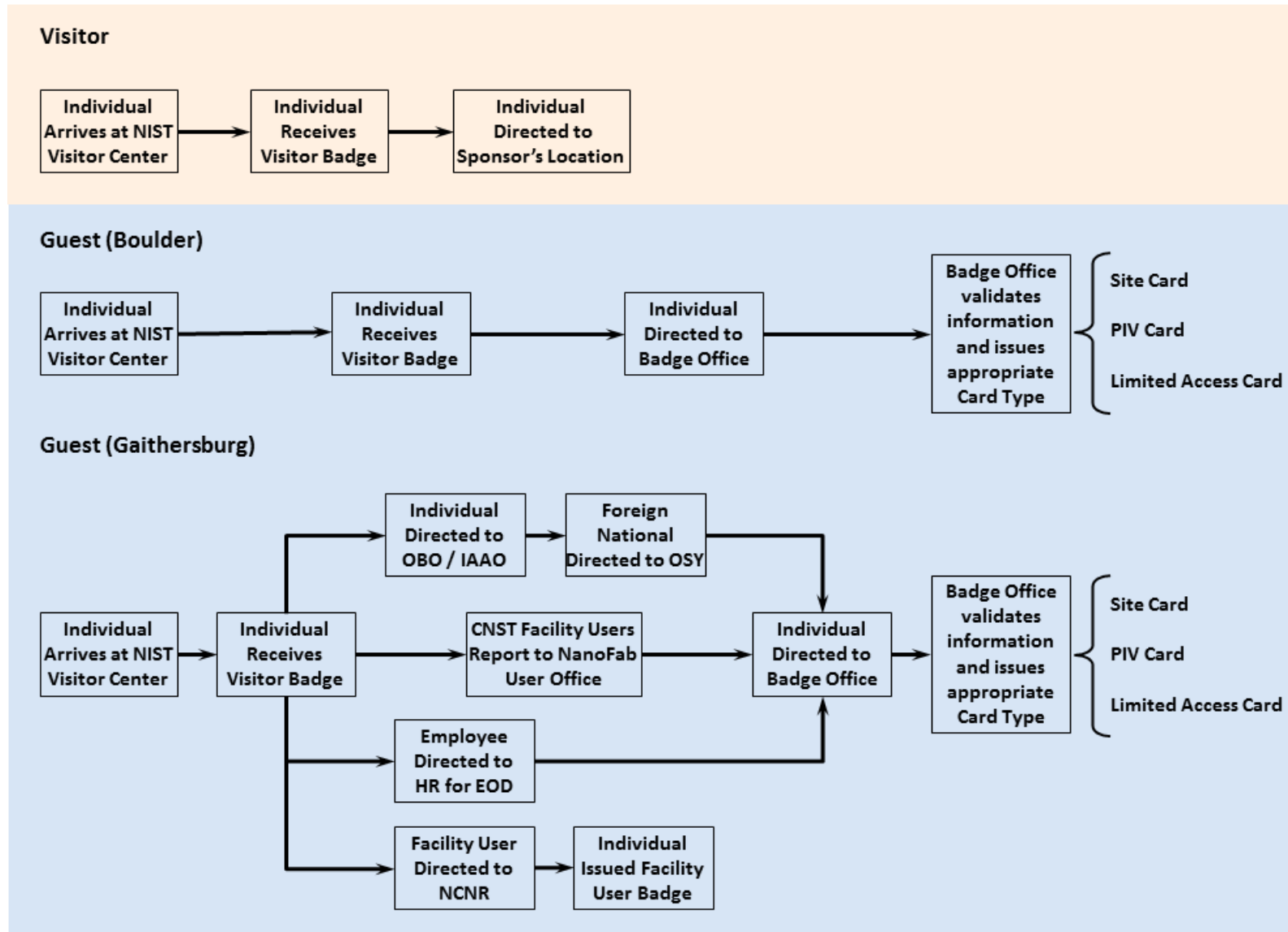
191 – OFPM Emergency Services Division (ESD)

APPENDICES

- A. NIST FAC Procedures
- B. Rules of Behavior
- C. Procedures for NOAA, NTIA and GSA (Boulder only)
- D. Revision History

APPENDIX A

NIST FAC Procedures



APPENDIX B

RULES OF BEHAVIOR FOR ALL CARD TYPES (FAC)

- The NIST FAC must be displayed fully to the Police Officer/Security Officer at all access gates and any other time you are challenged while on the NIST campus.
- All visitors/guests must display their White Visitor Card while on the NIST campus and must remain with their NIST sponsor/host at all times. NIST sponsors that do not maintain control of visitors while on site may lose their ability to further sponsor visitors to the site.
- If authorized for “security-hours” access, you must swipe in and out of the campus during these hours.
- The NIST FAC should only be utilized to access previously authorized areas. You agree not to attempt to access controlled areas unless properly authorized.
- You may NOT piggyback when entering an access controlled space, unless escorting visitors / guests.
- You may not share your assigned NIST FAC or associated PIN (for PIV cards) with anyone and must protect each appropriately. Individuals found in violation of this policy will be escorted off site immediately and denied access to NIST-administered sites.
- You must secure your NIST FAC to prevent loss / theft.
- You must use your PIV for logical access at all times in accordance with [N 6103.09](#).
- You must immediately report a lost or stolen NIST FAC to ESD, x2805. Once reported you will be required to complete a DN-42 form for submission to the ESD.
- The NIST FAC remains property of the Federal government and must be returned when you depart from NIST (i.e., separation, retirement, transfer, termination). It can be turned in to the Badge Office, the Police Services Group Office, or to one of the PSOs at the gate.

APPENDIX C

Procedures for NOAA, NTIA and GSA

Sponsors

- Prepare and submit appropriate form (CD-591 for affiliates) in accordance with security guidelines for visitors to the Boulder site. All forms are submitted via email to bouldervc@nist.gov.
- Submit appropriate Foreign National (FN) forms to Western Regional Security Office (WRSO) for processing and approval (DAO 207-12 Attachment 2 & 3 and Access Requirements Document).
- Inform visitors of the rules, regulations and responsibilities during their visit to the NIST Boulder site.

Visitor Center

- Provide the fingerprint card to the employee being fingerprinted to provide to the sponsor for submission to WRSO for processing.
- Process fingerprints for NOAA and NTIA between the hours of 10:00 am – 11:00 am and 2:00 pm – 4:00 pm Monday – Friday.
- Issue appropriate NIST FAC type to registered guests at the Boulder site.
- Direct visitors to the appropriate building.

Badge Office

- Issue appropriate NIST FAC type to guests to the Boulder site (applicable to NIST, NOAA, NTIA and GSA).
- Issue PIN numbers to childcare parent/guardian card holders after National Crime Information Center (NCIC) approval from Police Services Group.
- Issue site-access card and PIN (once proper forms have been completed and approved by WRSO).
- Enroll and activate PIV for NIST, NTIA & GSA along with PIN, when appropriate. NOAA CAC (Common Access Card) generated on site in the NOAA Badging office.
- Assign access level to card type according to security policy and procedures (as determined by CD-591 and Access Requirement Document).

APPENDIX D

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	01/05/14	Dan Cipra (M&O)	First Draft for access control
Update	06/20/14	Edward Mai (ESD)	Incorporated badging and access control into one procedural document
Update	10/01/15	Edward Mai (ESD)	Incorporated comments from various sources
Update	02/20/16	Edward Mai (ESD)	Updated based upon comments received by the DRB
Update	03/08/16	Edward Mai (ESD)	Updated from additional comments and responses.

Human Resources (HR) Management Policy

NIST P 3100.00

Effective Date: 6/26/2014

PURPOSE

To articulate NIST's commitment to delivering high quality human resources (HR) management services and oversight through:

- Partnering with clients to recruit, develop, manage, and retain a highly talented and diverse workforce;
- Continually improving systems and services to deliver better client solutions;
- Continually advancing staff capabilities to meet emerging HR needs of the Institute and the federal HR profession; and,
- Ensuring compliance with applicable laws and regulations, including the requirement to protect merit system principles.

SCOPE

This policy applies to all NIST federal employees.

LEGAL AUTHORITIES AND REFERENCES

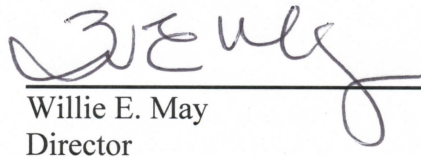
- [The National Bureau of Standards Authorization Act for Fiscal Year 1987](#), as amended, [15 U.S.C. 275](#) note
- [Executive Order 9830](#), Amending the Civil Service Rules and Providing for Federal Personnel Administration
- [Department Organization Order \(DOO\) 20-8, Director for Human Resources Management](#)
- [Department Administrative Order \(DAO\) 202-250, Delegations of Authority for Human Resources Management.](#)
- NIST Alternative Personnel Management System (APMS), [52 Fed. Reg. 37082 \(Oct. 2, 1987\)](#), as amended (see Appendix A for Federal Register Notices amending the APMS)

POLICY

It is NIST policy to follow applicable Office of Personnel Management and Department of Commerce policies and procedures that support and govern the development, management, administration, and coordination of HR programs at NIST, including the policies and procedures of the NIST APMS. This includes ensuring compliance with applicable laws and regulations that govern the full spectrum of federal human resources management.

The Director of the Office of Human Resources Management (OHRM) is responsible for defining and developing requirements, processes, procedures and operational policies to govern and guide personnel programs used in the delivery of NIST HR-related support and services.

The OHRM Director will ensure that compliance and quality of HR services are maintained through regular communication with clients, supervisory review of work products, audits, and training of HR and NIST staff, as appropriate.



Willie E. May
Director

7/25/15

Date

APPENDIX A

FEDERAL REGISTER NOTICES REGARDING THE NIST ALTERNATIVE PERSONNEL MANAGEMENT SYSTEM (APMS)

[52 Fed. Reg. 37082 \(Oct. 2, 1987\),](#)
[54 Fed. Reg. 21331 \(May 17, 1989\)](#)
[54 Fed. Reg. 33790 \(Aug. 16, 1989\)](#)
[55 Fed. Reg. 19688 \(May 10, 1990\)](#)
[55 Fed. Reg. 39220 \(Sept. 25, 1990\)](#)
[62 Fed. Reg. 54604 \(Oct. 21, 1997\)](#)
[70 Fed. Reg. 23996 \(May 6, 2005\)](#)
[73 Fed. Reg. 40500 \(July 15, 2008\)](#)
[74 Fed. Reg. 35841 \(July 21, 2009\)](#)
[74 Fed. Reg. 35843 \(July 21, 2009\)](#)
[76 Fed. Reg. 539 \(Jan. 5, 2011\)](#)
[76 Fed. Reg. 78889 \(Dec. 20, 2011\)](#)
[77 Fed. Reg. 36485 \(June 19, 2012\)](#)
[77 Fed. Reg. 48128 \(Aug. 13, 2012\)](#)
[77 Fed. Reg. 51518 \(Aug. 24, 2012\)](#)

Telework Program

NIST O 3102.00

Effective Date: 3/28/2012

PURPOSE

This Order defines the requirements of the National Institute of Standards and Technology (NIST) telework program. This directive complies with the Department of Commerce (DOC) Telework Program and Policy (10/15/2014) and replaces the NIST Administrative Manual Subchapter 10.27, Telework Program.

APPLICABILITY

This directive is applicable to all NIST Federal employees.

Where an employee requests telework as a reasonable accommodation, the Department of Commerce “Reasonable Accommodation for Employees or Applicants with Disabilities” (DAO 215-10) applies rather than this policy.

LEGAL AUTHORITY

- Telework Enhancement Act of 2010

REFERENCES

- U.S. Department of Commerce Telework Program and Policy (October 15, 2014).
- Office of Personnel Management Guide to Telework in the Federal Government (April 2011).
- Annual Telework Eligibility Notification and Updated Telework Policy Information for Federal Employees (Email from Director, Office of Human Resources Management to all NIST Federal Staff, December 4, 2014).
- Site Access During Site Closure and Delayed Openings (Directive Number O 2105).

REQUIREMENTS

NIST shall comply with the DOC Telework Program and Policy (10/15/14) and all other requirements as identified by NIST below.

Eligibility:

An employee shall be eligible to telework if:

- The employee is on a performance plan for at least 120 days; and

- The first-level supervisor has determined that the employee is performing at or above a contributor level.

An employee shall not be eligible to telework if:

- The employee has been officially disciplined for being absent without permission for more than five (5) days in any calendar year; or
- The employee has been officially disciplined for viewing, downloading or exchanging pornography, including child pornography, on a Federal Government computer or while performing official Federal Government duties.
- Except in emergency situations determined by the head of the agency, telework does not apply to any employee whose official duties require, on a daily basis:
 - Direct handling of secure materials determined to be inappropriate for telework;
 - On-site activity that cannot be handled remotely or at an alternate worksite.

Participation:

Participation requires:

- A written and signed agreement outlining the specific work arrangement (see Appendix A, NIST Telework Program, Employee/Supervisor Agreement);
- That the performance of the employee complies with the terms of the mandatory written agreement;
- That the employee has a complete and signed Performance Management Record (NIST 01) or Executive Performance Agreement in place for at least 120 days, and the supervisor has determined that the employee is performing at or above a contributor level;
- Completion of training, as required by the DOC Telework Program and Policy, by both the employee and the supervisor/manager prior to the implementation of a Telework Agreement;
- A completed and signed Alternative Worksite Safety Checklist -- if the worksite is in a private residence -- where all applicable questions were answered in the affirmative, or, if answered in the negative, confirmation that the employee will take all necessary corrective actions to eliminate any hazard prior to beginning telework (see Appendix B, Alternative Worksite Safety Checklist);
- Emergency contact information be incorporated as part of continuity of operations plans as appropriate.

An employee's telework privileges may be revoked if:

- The first-level supervisor determines that the employee's performance does not comply with the terms of the signed NIST Telework Program Employee/Supervisor Agreement.

An employee may elect to terminate his/her participation in the telework program at any time.

Telework Plans

An employee shall have the opportunity to choose between one of two telework options, subsequent to the concurrence of the first-level supervisor:

- Plan A:
 - The employee shall be limited to no more than 80 hours of ad hoc/unscheduled telework during a 12 month term.
 - The employee shall follow OU policies and procedures for requesting ad hoc/unscheduled telework.
 - The employee **shall not be required** to telework if NIST announces delayed arrivals, early dismissals, or closures.
 - The employee may change to Plan B at any time prior to reaching the 80-hour limitation.
- Plan B:
 - The employee shall be scheduled for regular/recurring telework as outlined in the NIST Telework Program Employee/Supervisor Agreement.
 - The employee **shall be required** to telework if NIST announces delayed arrivals, early dismissals, or closures.
 - Also includes employees who desire the option of ad hoc/unscheduled telework for more than 80 hours.
 - Employees performing less than 80 hours of ad hoc/unscheduled telework does not change the employee's election of Plan B.

Incidents at Telework Sites

Employees shall be covered under the Federal Employee's Compensation Act (FECA) if injured in the course of performing official duties at the alternative worksite.

An employee shall notify their line management of any incident (e.g., work-related injury, near-miss, property damage, etc.) according to Organizational Unit (OU) policies and procedures for doing so.

Upon notification, NIST may investigate the incident report that occurred at the alternative worksite.

NIST will not be liable for damages to an employee's personal or real property during the course of performance of official duties or while using NIST material in the employee's residence or elsewhere, except to the extent NIST is held liable by the Federal Tort Claims Act or the Military Personnel and Civilian Employees Claims Act.

Emergency Conditions

- Although a variety of circumstances may affect individual situations, the principles governing administrative leave, dismissals, and closing remain unchanged.
- If teleworking at a GSA telework center:

- Employees shall follow the arrival, dismissal, and closure procedures of the telework center regardless of NIST announcements of delayed arrivals, early dismissals, or closures.
- If the arrival, dismissal, and closure procedures of the telework center limit the employee's ability to perform their duties, the employee must notify his/her first-level supervisor and request administrative leave according to OU policies and procedures. First-level supervisors will consider requests for administrative leave on a case-by-case basis and will consult with the Office of Human Resources Management (OHRM) as necessary. Documentation in support of the request may be required.
- If teleworking from residence:
 - Employees shall be required to work during NIST delayed arrivals, early dismissals, and closures and will not normally be granted hazardous weather leave.
- Extenuating circumstances
 - If conditions at the telework site (e.g., power failure) affect the employee's ability to perform his/her duties, first-level supervisors will consider requests for administrative leave.
 - If conditions at NIST impact the ability to work at the telework site (e.g., the servers are shut down), employees at the telework site will be treated in the same manner as those working at NIST.

RESPONSIBILITIES

NIST Director

- Serves as final approval authority for the NIST Telework Program.

NIST Organizational Unit (OU) Directors

- Authorizes the expenditure of funds for telework.
- Ensures the development of an OU telework program tailored to meet the needs of their employees, in accordance with NIST's Telework Program.
- Ensures the consistent and appropriate implementation of the telework program within their OU:
 - Ensures that OU employees are not directed or coerced to participate in the telework program;
 - Ensures that telework agreements (Appendix A) are current and maintained by the Administrative Officers in the OUs and are available for review by the NIST Telework Coordinator.
- Ensures an annual evaluation of the telework program within their OU.

NIST Division Chiefs

- Review employee requests for participation in telework which have been disapproved by supervisors and the rationale for such decisions and for maintaining documented

approvals/disapprovals to facilitate the evaluation, reporting and monitoring of the telework program. The Division Chief will communicate any telework denials to the employee and to the NIST Telework Coordinator.

- Maintain a record of the number of employees participating in the telework program.
- Making decisions regarding whether to permit exceptions to telework procedures on a case-by-case basis and providing these to the NIST Telework Coordinator.

NIST Supervisors

- Reviewing the "Telework Assessment Tool" (Appendix B in the DOC Policy) with the employee to determine the appropriateness of the employee teleworking prior to the employee submitting a formal request to telework.
- Evaluating an employee's request to participate in telework in a timely manner.
- With advance notice of at least 24 hours, the supervisor or designee has the right to inspect the alternative worksite before the arrangement begins and at periodic intervals during the telework arrangement to ensure that the workspace is safe and that all equipment is adequately installed and performing properly.
- If telework is approved:
 - Orientating employees to the telework program and ensuring that employees new to telework complete training as required by the DOC Telework Program and Policy;
 - Completing training for first-level supervisors, as required by the DOC Telework Program and Policy;
 - Reviewing the employee's Telework Safety Checklist to ensure it is complete when warranted;
 - Informing employees of those work tasks they are expected to perform while in a telework status;
 - Monitoring and evaluating the employee's performance based on the employee's Performance Management Record (NIST 01) or Executive Performance Agreement and the Telework Agreement.
 - Ensuring that telework-ready employees receive the same treatment and opportunities as non-telework-ready employees (*e.g.*, work assignments, awards and recognition, development opportunities, promotions, etc.);
 - Ensuring that applicable policies and procedures are followed under a telework agreement with regard to removal of/accountability for government property, records and documents; and approval of overtime, leave, alternative work schedules, information security policies (particularly access/use, remote access, and mobile devices), etc.;

- Ensuring employees properly and timely report telework equipment in accordance with NIST processes, including annual renewal and monthly certification as requested by the property custodian or property accountability officer;
- Establishing communication requirements and methods to ensure the employee is kept informed of relevant information, performance expectations and progress, and is made aware of requirements to be available for contact by the supervisor, co-workers, customers, etc., including, but not limited to, scheduling staff or all-hands meetings on days and at times when the maximum number of employees are present at the regular worksites, and/or making arrangements for conference call connections for employees at alternative worksites;
- Ensuring accurate employee recordation of telework in the time and attendance system.
- Investigating employee reports of work-related injury or illness at the alternative worksite in much the same manner as would be the case for injury or illness at the traditional worksite;
- During emergency conditions, ensuring that employees working at alternative worksites are aware of their working status if the NIST campus is closed or employees are given early dismissal; and
- Terminating, modifying, or temporarily suspending telework agreements at any time for mission-related reasons (such as operational needs, changes in office priorities, vacancies or long-term leave of other employees in the office that cause office coverage issues, employee's failure to adhere to the terms and conditions of the agreement, employee conduct, or employee performance, in accordance with the law and any applicable Collective Bargaining Agreements (CBA), rather than personal reasons).
- If a telework request is approved, but restricted:
 - Ensuring that restrictions are based on sound business or mission-related criteria (such as operational needs, employee conduct, or employee performance, in accordance with the law and any applicable CBAs, rather than personal reasons).
- If a telework request is denied:
 - Ensuring that denials are based on sound business or mission-related criteria (such as operational needs, employee conduct, or employee performance, in accordance with the law and any applicable CBAs, rather than personal reasons); and
 - If a telework request is denied, supervisors are required to submit a copy of the original request and the written denial to their supervisor and to the NIST Telework Coordinator.

- Responding to requests for information or reporting requirements from the NIST Telework Coordinator in a timely manner.
 - The approving official must deny or immediately terminate the agreement, as applicable, if the employee fails to be eligible to telework due to the reasons set forth in 5 U.S.C. §§ 6502(a)(2) or (b)(3).

NIST Teleworking Employees

- Request to participate in the telework program (through submission of Appendix A: DN-27, National Institute of Standards and Technology Telework Program Employee/Supervisor Agreement)
- If telework is approved, adhering to the terms and conditions of the telework arrangements which includes:
 - Completing training, as required by the DOC Telework Program and Policy (this training does not need to be repeated unless otherwise instructed);
 - Completing the Alternative Worksite Safety Checklist if the telework site is a residence;
 - Maintaining a telework site that is free of distractions and obligations which would impair his/her ability to provide the same time and level of attention to the work product as when onsite;
 - Following all standards governing ethical behavior regardless of where or when work is performed;
 - Adhering to information security policies, particularly related to access/use, remote access, mobile devices, etc.;
 - Ensuring that records subject to the Privacy Act of 1974 or have Personally Identifiable Information (PII), and Business Identifiable Information (BII) are not disclosed to anyone except those who have been authorized access to such information in order to perform their duties.
 - Performing his/her duties and official responsibilities at a “Contributor” level or greater;
 - Maintaining reasonable care of all NIST-owned property and material;
 - Accurately recording their time each pay period as telework in all time and attendance records.
 - Covering any utility cost, including high-speed internet connection needed to gain access to NIST information technology (IT) systems, electricity, heating, and lighting used while teleworking at their home; and
 - Notifying line management of any incident (e.g., work-related injury, near-miss, property damage, etc.) according to OU policies and procedures for doing so.

- Initiating a grievance, if so desired, if telework is approved but restricted, denied, or revoked.
 - Telework-ready employees who are not covered by a negotiated grievance procedure (NGP) must use the administrative grievance procedure in DAO 202-771, "Administrative Grievance Procedure," to appeal issues relating to their telework status or other telework matters.
 - Employees covered by a NGP that does not specifically exclude this matter must use the applicable NGP.
- Employees who believe they are the victims of prohibited discrimination may utilize the Equal Employment Opportunity Commission complaint procedures or the negotiated grievance procedure, as appropriate.

NIST Telework Coordinator

- Provides guidance on NIST telework policy and procedures to employees and supervisors.
- Develops and implements a reporting system to capture metrics on telework participation, hours teleworked, terminations, and denials.
- Ensures that the NIST Telework Program is operating in compliance with laws, regulations, and DOC policies and procedures.

DIRECTIVE OWNER (DO)

170 – Office of Human Resources Management

APPENDICES

- A. NIST Telework Program Employee/Supervisor Agreement
- B. Alternative Worksite Safety Checklist
- C. Revision History

APPENDIX A

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY TELEWORK PROGRAM EMPLOYEE/SUPERVISOR AGREEMENT

The following constitutes an agreement on the terms and conditions of the Telework Program at http://inet.nist.gov/ohrm/directives/own_directive_telework.cfm between the employee and supervisor named below:

Section I - To Be Completed by Employee and Supervisor

Employee Name:

Organization: [organization name and division or group number]

Job Title or Description: [e.g., computer security research, IT assistance, etc.]

Position Title: [e.g., Supervisory Computer Scientist, etc.]

Employee Office Phone Number:

Supervisor's Name, Title and Phone Number:

Term of Agreement begins _____ and ends
_____.

1. Employee volunteers to participate in the Telework Program and agrees to adhere to the applicable guidelines and policies, including the "Terms and Conditions" identified below and the NIST Telework Directive set forth at http://inet.nist.gov/ohrm/directives/own_directive_telework.cfm. Employee agrees to participate in the following plan:

- ☐ Plan A
 - Limits Ad hoc/unscheduled teleworking to no more than 80 hours during a 12 month term
 - Employee **not** required to telework in weather-related closures
 - Employee can change to Plan B at any time prior to reaching the 80-hour limitation

OR

☐ Plan B

- Includes employees on a regular/recurring telework schedule
- Also includes employees who desire the option of ad hoc/unscheduled telework more than 80 hours
- Employees performing less than 80 hours of ad hoc/unscheduled telework does not change the employee's election of Plan B
- Employee **is required** to telework in weather-related closures

2. Description of work to be performed by Employee at Alternative Worksite (e.g., updating policy, preparing briefing materials and talking points, etc.):
-

3. Employee's official duty station is at the National Institute of Standards and Technology (NIST). The alternative worksite is:

☐ The employee's home [address and telephone number].

OR

☐ Other [address and telephone number].

4. Necessary Equipment: List the equipment needed to perform work at the Alternative Worksite, including any government-furnished special telecommunications technology required, installation cost and data, and periodic costs.
-

5. Government-Furnished Equipment: List any government-furnished equipment required, the NIST ID# of each piece of loaned equipment, any installation cost and data, and any periodic costs.
-

6. Personal Equipment: List any personal equipment to be used by Employee.
-

7. Employee's Work Schedule Including AWS Day Off (If Applicable):

-
8. Conventional Office: When not on travel or leave, the employee will be at the conventional office a minimum of _____ days per week. The specific day(s) of the week will be determined as agreed upon by the supervisor and the employee. The work schedule for these days will be the work hours as appropriate under the current work schedule in effect for the employee on the date of initiation of this agreement.
 9. Alternative Worksite: When not on travel or leave, the employee will be at the alternative worksite a maximum of _____ day(s) per week. The days of the week the employee will be at this alternative worksite may vary depending on the work being done. The specific day(s) of the week will be determined as agreed upon by the supervisor and the employee on an ad hoc short-term basis to accommodate special needs.
 10. COOP employee: If an employee is designated as an “emergency employee” or part of COOP they are expected to work during a COOP event such as a national or local emergency, or a COOP exercise.
 11. Meetings and Unanticipated Work Requirements - Employee agrees to report to the official duty station within _____ hours of notification by a supervisor or manager of an unanticipated work requirement requiring his or her physical presence at the official duty station. The employee also agrees to adjust his or her scheduled hours at the alternate workstation to accommodate occasional meetings and other activities as needed.

Section II – TERMS AND CONDITIONS

Voluntary Participation – The employee voluntarily agrees to work at the approved alternative workplace indicated above and to follow all applicable policies and procedures. The employee recognizes that the telework arrangement is a privilege, not a right.

Salary and Benefits - The supervisor and employee agree that a telework arrangement is not a basis for changing the employee's salary or benefits.

Official Duties - The employee agrees not to conduct personal business while in an official duty status at the alternative work place (e.g., caring for dependents or making home repairs, etc.).

Time and Attendance - Employee's timekeeper will have a copy of the employee's telework schedule. The supervisor and employee are responsible for ensuring the accuracy of time and attendance reported for work at the official duty station and the alternative workplace.

Leave - Employee will follow the established office procedures for requesting and obtaining approval of leave.

Overtime – If Employee is “non-exempt” under the Fair Labor Standards Act, Employee agrees to work overtime only when approved in writing or via webTA and in advance by the supervisor and understands that claimed overtime work without such approval may result in termination of the telework privilege.

Office Coverage - The employee and supervisor will consider and make necessary arrangements with other staff members to ensure appropriate coverage of the employee's routine area of responsibility that might occasionally require a physical presence during regular NIST business hours.

Alternative Worksite Costs - The employee understands that the Government will not be responsible for any operating costs that are associated with the use of the employee's home as an alternative worksite, for example, home maintenance, insurance or utilities. (See discussion on “Equipment/Supplies” for covered costs). By participating in the telework program, the employee does not relinquish any entitlement to reimbursement for authorized expenses incurred while conducting business for the government, as provided for by statute and implementing regulations.

Equipment/Supplies - The employee agrees to protect any government-owned equipment and to use the equipment only for official purposes. Should the agency agree to provide government-owned equipment to the employee for the purposes of telework, the agency may install, service, and maintain such equipment, as necessary. The employee agrees to install, service, and maintain any personal equipment used. The agency agrees to provide the employee with all necessary office supplies and also reimburse the employee for business-related long distance telephone calls. If employee borrows government equipment, employee will borrow the

equipment in accordance with applicable procedures. If employee, at his or her option, provides his or her own equipment, employee is responsible for purchasing, servicing, and maintenance costs. The government will not be liable for reimbursing employees for such costs. Form NIST-393 Equipment Loan Authorization, Receipt, and Property Pass is to be completed and maintained on file with the NIST Property Office.

Security - The employee agrees to follow all existing security policies and procedures, including IT security. Employee agrees to ensure that government-furnished equipment, resources, and services are used in accordance with NIST policies. Employee also agrees to safeguard government data to prevent unauthorized access, release, or alteration. Decisions regarding the proper use and handling of Sensitive Information will be made by the individual supervisors who permit employees to work at home or an alternative worksite. Supervisors and teleworkers agree that Highly Sensitive Information will not be worked on at any off-site location.

Liability - The employee understands that the government will not be held liable for damages to his/her personal or real property while he/she is working at the approved alternative worksite, except to the extent the government is held liable under the Military Personnel and Civilian Employees Claims Act and the Federal Tort Claims Act.

Alternative Worksite Inspection - The employee agrees to permit the Government to inspect the alternative worksite during the employee's normal telework working hours to ensure proper maintenance of Government-owned property and conformance with safety standards with a 24-hour notice. This is in addition to the Telework Safety Checklist that the employee may be required to complete (see "Work Area").

Work Area - An employee working at a private residence agrees to provide a designated work area adequate for performance of official duties and must complete the Telework Safety Checklist (see Appendix B).

Injury Compensation - Employee understands that he/she is covered under the Federal Employees Compensation Act if injured in the course of actually performing official duties at the alternative worksite. The employee agrees to notify his/her supervisor immediately of any accident or injury that occurs at the alternative workplace and to complete any required forms. The supervisor agrees to investigate such a report as soon as possible.

Work Assignments/Performance - The employee agrees to complete all assigned work according to guidelines and standards in the employee's Telework Agreement and Performance Management Record (NIST 01) or Executive Performance Agreement. The employee and supervisor agree to exercise good communication skills and work cooperatively to obtain a common understanding of expectations and desired results and set reasonable and measurable objectives for work to be accomplished. The employee agrees to provide regular reports if required by the supervisor to help judge performance. The employee understands that a decline in performance may be a basis for terminating or modifying the telework arrangement.

Disclosure - The employee agrees to protect government records from unauthorized disclosure or damage and will comply with requirements of the Privacy Act of 1974, 5 USC 552(a), and those outlined in the DOC's Telework Program section "Privacy Act, Sensitive, and Highly Sensitive Information" located at http://hr.commerce.gov/s/groups/public/@doc/@cfoasa/@ohrm/documents/content/prod01_010437.pdf, page 18.

Standards of Conduct - The employee agrees that he/she is bound by official standards of conduct while working at the alternative worksite.

Cancellation - The employee understands that the organization may cancel the telework arrangement and instruct him/her to resume working at the office at any time. If the employee elects to voluntarily withdraw from the program, he/she is expected to give sufficient notice so that arrangements can be made to accommodate his/her return to a regular work schedule, and he/she must complete the Telework Termination Form in Appendix D of the DOC Policy. An employee on Plan A can change to Plan B at any time prior to reaching the 80-hour limitation.

Compliance with This Agreement - The employee's failure to comply with the terms of this agreement may result in the termination of this agreement and the telework arrangement. Failure to comply also may result in disciplinary action against the employee if just cause exists to warrant such action.

Employee's Certification - By signing this agreement, the employee certifies that he/she has read the Terms and Conditions of this agreement and agrees to follow the policies and procedures outlined in them as well as attached OU and/or division-specific telework documents, if applicable.

Supervisor's Certification - By signing this agreement the immediate supervisor of the employee certifies that the position of the employee is suitable for telework and that the employee is personally eligible for telework.

Section III – Certifications, Approval/Disapproval, and Signatures

I certify that I have completed the Telework 101 for Employees course offered in the Commerce Learning Center (CLC): (initial)_____

I certify that I have read and agree to the Terms and Conditions listed below and the NIST Telework Directive set forth at: (initial)_____

Employee's Signature and Date:_____

Approved: () Disapproved: () Reason Not Approved:

I certify that the employee's most recent rating of record is a Level 3 (i.e., Contributor or higher) and that I have completed the Telework 101 for Supervisors course offered in the CLC: (initial):_____

Supervisor's Signature and Date: _____

APPENDIX B

ALTERNATIVE WORKSITE SAFETY CHECKLIST

This checklist is to be completed only if the proposed alternative worksite is in a private residence. This checklist is designed to assess the overall safety of the designated work area of the alternative worksite. Each employee should read and complete the self-certification safety checklist. Upon completion, the checklist should be signed and dated by the employee and submitted to the immediate supervisor.

Employee Name: _____

Location, Address, and Telephone of Alternative Worksite:

Describe the Designated Work Area:

1. Are stairs with four or more steps equipped with handrails? ☐ Yes ☐ No ☐ N/A
2. Are aisles, doorways, and corners free of obstruction? ☐ Yes ☐ No ☐ N/A
3. Are file/storage cabinets arranged so that open doors/drawers do not create obstacles? ☐ Yes ☐ No ☐ N/A
4. Is the office space neat, clean, and free of combustibles? ☐ Yes ☐ No ☐ N/A
5. Are phone lines, electrical cords, and surge protectors secured under a desk or alongside a baseboard? ☐ Yes ☐ No ☐ N/A
6. Are circuit breakers/fuses in the electrical panel properly labeled? ☐ Yes ☐ No ☐ N/A
7. Is electrical equipment free of recognized hazards that could cause physical harm (e.g., frayed, loose and/or exposed wires, bare conductors, etc.)? ☐ Yes ☐ No ☐ N/A
8. Does the building electrical system permit grounding of equipment (i.e., have three-prong receptacles)? ☐ Yes ☐ No ☐ N/A
9. Is there a smoke alarm and clear access to a fire extinguisher? ☐ Yes ☐ No ☐ N/A

By signing this document, the employee certifies that all of the above applicable questions were answered in the affirmative, or, if answered in the negative, that the employee will take all necessary corrective actions to eliminate any hazard prior to beginning telework.

Employee Signature and Date:

APPENDIX C

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/15/2011	Mary Willett	Initial Draft
Final Draft	2/9/2012	Mary Willett	Incorporated Changes from Melissa and OGC.
Final	2/22/2012	Dan Cipra	Incorporated format changes and prepared for publishing
Rev. 1	5/9/13	Mary Willett	Revised NIST Telework agreement to reflect revised February 2013 DOC Telework Policy (applies to NIST bargaining unit as well as non-bargaining unit employees)
Rev. 2	11/26/14	Audrey Terry and Mary Willett	Revised NIST Directive and Telework agreement to reflect revised October 2014 DOC Telework Policy
Rev 2.1	6/12/2015	Dan Cipra	Incorporated all updates from OGC relating to the new DOC policy.

NIST NRC Postdoctoral Research Associateship Program

NIST O 3105.00
Effective Date: 5/9/2016

PURPOSE

This directive defines the requirements and responsibilities for the National Institute of Standards and Technology (NIST) National Research Council (NRC) Postdoctoral Research Associateship (NIST NRC Postdoc) Program, carried out in conjunction with the NRC. The NIST NRC Postdoc Program provides opportunities for research and advanced training for recent doctoral graduates of unusual ability and promise through their participation in NIST research programs in fields including chemistry, physics, materials science, mathematics, computer science, and engineering.

APPLICABILITY

This directive is applicable to all NIST employees involved with administrative processing and support for NIST NRC Postdocs at NIST-Gaithersburg, NIST-Boulder, and at sites that NIST shares with other organizations and to the NIST NRC Postdocs.

REFERENCES

- NIST PR 3105
- [15 U.S.C. 278g-2](#), NIST Postdoctoral Fellowship Program
- [Federal Travel Regulation 302-3](#)
- [NRC Research Associateship Program](#)¹

NIST-REQUIRED FORMS

- [OF-306](#), Declaration for Federal Employment
- [SF-52](#), Request for Personnel Action
- [CD-150](#), Request for Authorization of Travel and Moving Expenses
- [CD-29](#), Travel Order

¹ Historical information regarding the program can be found in "Approaches for Evaluating the NRC Resident Research Associateship Program at NIST", National Research Council, 2007, Board for Higher Education and Workforce, John Sislin, ed., Washington, D.C., The National Academies Press, and in "Assessment of the NRC NIST Postdoctoral Research Associateship Program", Westat, Keith MacAllum, Gary Silverstein, *et. al.*, Westat, 2012.

- [CD-370 Travel Voucher](#)
- [CD-26/NIST-598](#), Separation Clearance Certificate with NIST-598 Supplemental Sheet

DEFINITIONS

Central funds – refers to appropriated NIST funds designated for the NIST NRC Postdoc Program; funds are Scientific and Technical Research and Services (STRS) distributions from International and Academic Affairs (IAAO).

NIST NRC Postdoctoral Research Associates (NIST NRC Postdocs) – refers to those individuals hired by NIST through the NIST NRC Postdoc program as NIST term employees. The term “Associate” is used rather than “Fellow,” as this is the traditional term for those in the NRC Research Associateship Program.

International and Academic Affairs Office (IAAO) – refers to the NIST office that has responsibility for administering the NIST NRC Postdoc Program.

Laboratory/Center Review (LCR) form – refers to the NRC form that the NIST NRC Postdoc Program advisers fill out and sign during the application process and return to IAAO with an appropriate Division Chief (or equivalent) endorsement. A direct link to this on-line form is provided by NRC to each adviser within one week following the deadline for application, and is linked to the respective applicant.

Laboratory Program Representative (LPR) – refers to the IAAO staff member who is recognized as the official NIST representative to the NRC Postdoctoral Research Associateship Program, and whose endorsement and/or signature is required on forms sent to the NRC.

Travel Group – refers to the NIST office that has responsibility for the oversight of travel by NIST employees or others traveling on Government funds on behalf of NIST.

REQUIREMENTS

- NIST is directed by 15 U.S.C. 278g-2 to conduct a postdoctoral fellowship program, known as the NIST NRC Postdoc Program, in the same manner as the National Academy of Sciences/National Research Council Postdoctoral Research Associateship Program that was in effect prior to 1986, now known as the National Academies of Sciences, Engineering and Medicine/National Research Council. The program shall include no fewer than twenty or more than 120 new fellows per fiscal year.
- This program shall be open only to citizens of the United States, and applicants must have held their doctoral degree less than five years at the time of application deadline (1 February or 1 August). Qualified applicants will receive consideration without regard to race, creed, age, color, sex, sexual orientation, national origin, or disability.
- A majority of the NIST NRC Postdoc positions shall be supported from a central fund managed by IAAO. Additional NIST NRC Postdocs may be funded by the NIST Laboratories in accordance with selection procedures specified by IAAO together with the NIST Director (or designee) each competition cycle.

- The formal hiring of a NIST NRC Postdoc shall be contingent on meeting security and suitability requirements, which are confirmed through the NIST Office of Human Resources Management (OHRM).
- All incoming NIST NRC Postdocs must have completed all requirements for the doctoral degree prior to beginning their tenure for the program, and all males born after December 31, 1959 must have registered with the Selective Service System or have an exemption.
- Appointments of all NIST NRC Postdocs, whether supported from the central fund or from NIST Laboratory funds, shall be for a total working time of no more than two years, as mandated by their term appointments.
- NIST NRC Postdocs are required to complete a final report at the end of their tenure.

RESPONSIBILITIES

IAAO Education Program representative or designee

- Acts as the LPR for the NIST NRC Postdoc program.
- Serves as the point of contact and resolves issues identified by the NRC, NIST NRC Postdoc advisers, potential applicants, applicants, awardees, the postdoctoral associates, the NIST Budget Division, Administrative Officers, and NIST management.
- Acts as the Contracting Officer's Representative (COR) (must be delegated by the cognizant Contracting Officer), for the contract with the National Academy of Science/NRC Research Associateship Program Office for the NIST NRC Postdoc Programs.
- Maintains a database of NIST NRC Postdocs.
- Acts as an arbitrator when an agreement on changes or modifications to the originally proposed research cannot be reached.
- Coordinates any other activities deemed necessary for the program.

IAAO Administrative Officer (assigned to the NIST NRC Postdoc Program)

- Sets up budget projects, as needed, and tracks charges of relocation and labor costs for NIST NRC Postdocs that are centrally funded.
- Coordinates with the LPR regarding charges to the contract and relocation and labor costs related to the Postdoctoral Associates that are centrally funded.
- Coordinates financial information relating to new and departing NIST NRC Postdocs.
- Reviews and signs off on [CD-29](#) and [CD-150](#) forms for new NIST NRC Postdocs that are centrally funded, if relocation reimbursement is requested.
- Provides information, upon request, on the status of the central funds.

- Requests and collects a final report from each NIST NRC Postdoc prior to their completion of their postdoc tenure. The report should include a summary of their research work, publications, presentations, and other professional activities.

Administrative Officers (AOs) or designee

- Informs IAAO of information relating to the start and end dates of the terms of their NIST NRC Postdocs.
- Collects the necessary paperwork associated with hiring an incoming NIST NRC Postdoc and sends it to the Division's Human Resources Specialist.
- Sets up budget projects, as needed, and tracks charges of relocation and labor costs for NIST NRC Postdocs that are laboratory funded.
- Ensures the IAAO Administrative Officer is included on the routing list for all CD-150 forms for NIST NRC Postdoc travel.
- If relocation reimbursement costs are requested for centrally funded NIST NRC Postdocs, sends the CD-150 and CD-29 for review and approval to the IAAO AO. Also sends a copy of the CD-370 to the IAAO AO once completed.
- NOTE: The IAAO AO only needs to review and receive copies of the documents (CD-29, CD-150, and CD-370) if the NIST NRC Postdocs are centrally funded.
- Informs LPR and IAAO Administrative Officer of any changes in NIST NRC Postdoc status.

Office of Human Resource Management (OHRM)

- Collects the necessary paperwork from the appropriate AO from the NIST Laboratories related to the hire of an incoming NIST NRC Postdoc.
- Confirms that the incoming NIST NRC Postdoc has met security and suitability requirements.
- Completes the remainder of the required paperwork and tasks in the hiring process with the Division AO, including notification of the official start date.
- Sends a copy of the official offer letter for the incoming NIST NRC Postdoc to IAAO and Division AOs.
- Ensures IAAO has signed off on the separation forms (NIST-598) for NIST NRC Postdocs leaving NIST after finishing their tenure.

Travel Group

- Ensures compliance of NIST NRC Postdoc relocation and travel with Federal Travel Regulation 302.
- Ensures that the IAAO AO has reviewed and approved CD-150 and CD-29 for centrally funded NIST NRC Postdoc relocation.

NIST NRC Postdoc

- Furnishes all information as requested by IAAO and AOs, or their designees.
- Informs their adviser, as well as their AO, of the planned starting and ending dates.
- Completes a final report, as mandated by IAAO and NRC, with information and statistics on their postdoctoral tenure.

DIRECTIVE OWNER

101 – International and Academic Affairs Office (IAAO)

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	3 Oct 2012	Susan Heller-Zeisler (IAAO)	Original Draft from Admin Manual 10.22
Rev. 01	4 Oct 2012	Dan Cipra (M&O)	Reformatted to DMS template
Rev. 02	29 Mar 2013	Susan Heller-Zeisler (IAAO)	Made corrections as discussed with DC, submitted to Chief Counsel Office
Rev. 03	5 May 2014	Susan Heller-Zeisler	Received comments from H. Wixon, M. Liebermann, Chief Counsel Office
Rev. 04	22 May 2014	Susan Heller-Zeisler (IAAO)	Received draft directive back from M&O to resubmit under the new guidance.
Rev. 05	4/2/2015	Dan Cipra	Split up the Order and created this procedure.
Rev. 06	11/18/2015	Susan Heller-Zeisler (IAAO)	Further edits on order and procedure as necessary.
Rev 07	1/4/2016	Susan Heller-Zeisler	Added edits from Travel Group
Rev. 08	3/1/2016	Susan Heller-Zeisler	Added AO edits
Rev. .09	4/27/2016	Claire Saundry	Updated based on DRB Comments
Rev. .10	5/3/2016	Susan Heller-Zeisler	Final DRB updates from meeting.

NIST NRC Postdoctoral Research Associateship Program

NIST PR 3105.01
Effective Date: 5/9/2016

PURPOSE

This directive defines the procedures for the National Institute of Standards and Technology (NIST) National Research Council (NRC) Postdoctoral Research Associateship (NIST NRC Postdoc) Program, carried out in conjunction with the NRC. This includes the application, review, selection, on-boarding, tenure, and separation processes, as well as special circumstances.

APPLICABILITY

This directive is applicable to all NIST employees involved with administrative processing and support for NIST NRC Postdocs at NIST-Gaithersburg, NIST-Boulder, and at sites that NIST shares with other organizations, and to the NIST NRC Postdocs.

REFERENCES

- NIST O 3105, NIST NRC Postdoctoral Research Associateship Program (TBD)
- [National Research Council Research Associateship Programs](#)
- [SF-52, Appointments and Renewals/Postdocs](#)
- [Federal Travel Regulation \(FTR\) 302-3, Table A: Assigned to First Official Station in the Continental United States \(CONUS\)](#)
- [15 United States Code \(U.S.C.\) 278g-2](#) Post-Doctoral Fellowship Program

FORMS:

- [OF-306, Declaration for Federal Employment](#)
- [CD 150 Request for Authorization of Travel and Moving Expenses](#)
- [CD 29 Travel Order](#)
- [CD 126/NIST-598, Separation Clearance Certificate,](#)

BACKGROUND

NIST participates in two of the four competition cycles (termed “competitions”) organized by the NRC Research Associateship Programs (RAP) Fellowship Office for Postdoctoral Research Associates each year. For applicants to the NIST NRC Postdoc Program, applications are due February 1 and August 1.

A majority of the NIST NRC Postdoc positions are supported from a central fund managed by the International and Academic Affairs Office (IAAO). IAAO serves as the NIST Laboratory Program Representative (LPR) for the NIST NRC Postdoc Program.

NIST Laboratories have the option of supporting additional NIST NRC postdocs within the limits of the total number of allowable positions as per 15 U.S.C. 278g-2.

To be eligible, an applicant must meet the criteria listed in the requirements section of NIST O 3105.00, and the [eligibility section](#) on the NRC RAP website, and must submit the completed application package to the NRC according to the [instructions](#).

PROCEDURES

Application Process:

As part of the application process, administered by the NRC RAP Fellowships Office¹, an applicant:

- identifies a NIST staff member as a potential research adviser for the proposed work; and
- typically contacts the potential NIST advisor in advance of submitting the application.

NIST staff members:

- prepare research opportunities for inclusion on the NRC RAP website according to the [instructions](#), and review and update opportunities annually;
- may act as NIST NRC Postdoc advisors according to the [guidelines](#);
- may communicate with potential candidates during application process, but may not write the research application proposal; and
- must complete a section of the Laboratory Center Review (LCR), which is an on-line review form, for each of their applicants.

Division Chief, or equivalent:

- must endorse the LCR to ensure NIST commitment to support the research proposed by the applicant.

IAAO:

- obtains the necessary approval from the relevant Division Chief (or equivalent) via email; and
- endorses the LCR.

¹ The information on the application process is found at the National Academies Research Associateship Program Fellowships Office website, <http://sites.nationalacademies.org/pga/rap/>.

Review Process

Once the technical reviews have been completed, NRC RAP sends IAAO list of applicants in rank order.

IAAO:

- makes a recommendation on the number of positions that can be supported in each competition based on the status of the central fund;
- makes recommendations² to the NIST Associate Director for Laboratory Programs (ADLP), or his/her designee, concerning automatic offers and the distribution of positions amongst the NIST Laboratories;
- drafts the selection procedure, specific to each competition cycle, for approval by the NIST ADLP, or designee; and
- issues the approved selection procedure, list of applicants in rank order, and ratings information to the Laboratory Directors for each competition cycle.

NIST ADLP, or designee:

- decides the distribution of postdocs between the Laboratories; and
- approves the selection procedures which are specific to each competition cycle.

Additional NIST NRC Postdocs may be funded by the NIST Laboratories in accordance with the selection procedures defined for that competition.

The total number of NIST NRC Postdocs hired as NIST term employees per year, central and Laboratory-supported combined, shall not exceed the maximum as noted in [15. U.S.C. 278g-2 Post-doctoral Fellowship Program](#).

Selection Process

Laboratory Directors, or their designees:

- select the candidates for their Laboratories in accordance with the selection procedures for that competition; and
- communicate the names of their selected appointees to IAAO.

IAAO:

- sends letter of acceptance to each of the selected candidates; and
- at the end of the selection process, sends letters to those applicants not selected, advising them that they were not accepted.

² The normal recommendation for automatic offers to applicants whose score from the NRC panel review is greater than 96 out of the possible total of 100. The normal recommendation for the allocation of the remainder of the slots is by pro rating the number of applicants per Laboratory scoring a NIST-rated B+ or above, where then lowest B+ score is 87.0.

On-boarding Process

Prior to beginning tenure, the incoming NIST NRC Postdoc must:

- complete and submit to IAAO form [OF-306](#), Declaration for Federal Employment;
- submit to IAAO official university transcripts;
- provide current resume or curriculum vitae to IAAO;
- send IAAO a formal acceptance letter;
- provide documentation to IAAO of registration with the Selective Service System, or a written exemption (only for males born after December 31, 1959);
- meet security and suitability requirements, which are confirmed through the NIST office of human resource management (OHRM); and
- complete all requirements for the doctoral degree.

Prior to beginning tenure, IAAO:

- retains copies of relevant information for its records; and
- sends originals to the appropriate NIST administrative staff, *e.g.* the Division Administrative Officer (AO) or their designee.

Prior to beginning tenure, the Division AO or their designee:

- coordinates with the incoming NIST NRC Postdoc to complete the remainder of the required paperwork associated with the hire, following the guidelines of the NIST Office of Human Resource Management (OHRM) under [SF-52, Appointments and Renewals, Postdocs](#); and
- sends all the required documents to the appropriate OHRM Specialist.

Once all procedures are completed, the OHRM Specialist sends the official offer letter to the incoming NIST NRC Postdoc with a copy to IAAO and to the Division AO.

Incoming NIST NRC Postdocs may be authorized and reimbursed for expenses incurred during relocation travel (*i.e.*, transportation, per diem, and shipment of household goods). The regulations as outlined in the [Federal Travel Regulation \(FTR\) 302-3, Table A: Assigned to First Official Station in the Continental United States \(CONUS\)](#) apply when authorizing such travel.

Limits on central funding for the relocation expenses of centrally funded NIST NRC postdocs - for example, the maximum amount in transportation and moving expenses per postdoc and the postdoc's eligible accompanying family members - are given at the beginning of each fiscal year in a funding memo issued by IAAO.

Any expenses that a Laboratory wishes to authorize over the maximum amount in the funding memo for an incoming centrally funded postdoc must be stated in Section VII, the remarks section of [CD-150](#), and an appropriate laboratory project/task code and organization code must be noted for the extra amount.

All relocation expenses will be paid in accordance with the established allowances in the FTR 302-3.

Real estate transactions will not be authorized under any circumstances for NIST NRC Postdocs.

The authorization of temporary quarters may be authorized by the approving official on a case-by-case basis.

By signing the [CD-150](#), the NIST NRC Postdoc agrees to remain in the employment of the United States Government for twelve (12) months following the effective date of appointment. If the NIST NRC Postdoc violates this agreement, any relocation payments shall be recoverable from the NIST NRC Postdoc as a debt due to the United States Government.

The IAAO AO assigned to the NIST NRC Postdoc Program must sign off on the [CD-150](#) form prior to proceeding with the [CD-29](#). This signature will be located near the bottom of Section VII Justification/Remarks, and will follow any narrative regarding the [CD-150](#).

Following approval of the [CD-150](#) and accompanying paperwork, the IAAO AO must also approve the [CD-29](#) form in the role of Funds Certifying Officer (CD-29, Section 10B).

A copy of the final travel order and travel voucher must be provided to the IAAO AO, when these become finalized.

After final vouchers are submitted, all expenses over the maximum allowed amount will be charged to the sponsoring Division via a cost correction completed by the IAAO AO. Please note that, during this process, all documents should be hand-carried, sent by encrypted email, or faxed to maintain information protection.

Tenure

Appointments of all NIST NRC Postdocs, whether supported from the central fund or from Laboratory funds, are for a total working time of no more than two years, as mandated by their term appointments.

It is expected that NIST Laboratory Director and Division Chief, or equivalent will support the NIST NRC Postdoc's research as submitted to the NRC, and this support shall be confirmed by an appropriate endorsement (*e.g.* Division Chief, or equivalent) on the LCR.

Major changes or modifications to the proposed research should only occur if ALL parties (NIST NRC Postdoc, Adviser, and NIST Laboratory Director or designee, and Division Chief, or equivalent) are in agreement. If an agreement to such changes or modifications cannot be reached, IAAO shall act as arbitrator.

For all NIST NRC Postdocs (centrally funded or Laboratory funded), there shall be \$3000 dedicated travel support per tenure year. Travel funds are to be used for travel to meetings and conferences to disseminate research results and develop professional networks.

Each NIST NRC postdoc is expected to participate in one or two appropriate professional meetings each year.

Travel funds may not be used for other object expenses.

IAAO AO must be included in the travel manager routing for centrally funded NIST NRC Postdocs, and, when finalized, a copy of the final travel order and travel voucher must be provided to the IAAO AO.

In addition to travel support, the individual Divisions/Groups are expected to provide a minimum of \$2500 of other objects money per NIST NRC postdoc to support research³.

Special Circumstances

Change of NIST Research Adviser

A change in NIST research advisor may be made with the agreement of the NIST NRC Postdoc, the current and potential new advisers, the Division Chief, or equivalent, and Laboratory Director, or designee. IAAO shall be informed through Memorandum prior to a change taking place.

Extended leave

If a situation arises where the NIST NRC Postdoc needs to request extended leave beyond that accrued, Leave-Without-Pay (LWOP) may be utilized through a Memorandum from the Division Chief, or equivalent, through the Laboratory Director and the Group Leader of the NIST NRC Postdoc, to IAAO.

Approval by IAAO is granted on a case-by-case basis.

IAAO shall forward the approved/disapproved Memo to OHRM for their records, and inform the NIST NRC Postdoc as well as the Division of the determination.

If approved, the Division AO will complete and forward the necessary documents for the leave to OHRM, following the appropriate procedure for leave documentation. OHRM will complete the personnel action for the extended leave.

The amount of LWOP will be added to the NIST NRC Postdoc's term to extend their tenure date, but in all instances, the total working time may not exceed two years.

Separation Process

If a NIST NRC Postdoc departs NIST prior to completing the full two-year term, a notice of resignation must be submitted to IAAO at least 14 days in advance.

Prior to the end of tenure, the NIST NRC Postdoc must submit a final report to IAAO. This report is required whether or not the NIST NRC Postdoc remains at NIST in another capacity, departs before the full two-year term is completed, or remains for the full two-year term.

The format of the report is available at:

http://sites.nationalacademies.org/PGA/RAP/PGA_046585 and/or may be obtained from IAAO.

³ The requirement that OUs commit these funds for travel and other object funds was confirmed in the memorandum dated July 13, 2011 from the NIST Associate Director for Laboratory Programs (ADLP).

If the NIST NRC Postdoc departs from NIST at the end of postdoc tenure or before the end of the two-year term, the LPR in IAAO must sign the [NIST-598, Separation Clearance Certificate](#), prior to departure, acknowledging receipt of the final report. The NIST-598 shall not be finalized until IAAO has signed.

DIRECTIVE OWNER

101 – International and Academic Affairs Office (IAAO)

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	3 Oct 2012	Susan Heller-Zeisler (IAAO)	Original Draft from Admin Manual 10.22
Rev. 01	4 Oct 2012	Dan Cipra (M&O)	Reformatted to DMS template
Rev. 02	29 Mar 2013	Susan Heller-Zeisler (IAAO)	Made corrections as discussed with DC, submitted to Chief Counsel Office
Rev. 03	5 May 2014	Susan Heller-Zeisler	Received comments from H. Wixon, M. Liebermann, Chief Counsel Office
Rev. 04	22 May 2014	Susan Heller-Zeisler (IAAO)	Received draft directive back from M&O to resubmit under the new guidance
Rev. 06	4/2/2015	Dan Cipra	Split up the Order and created this procedure.
Rev. 07	11/18/2015	Susan Heller-Zeisler (IAAO)	Further edits on the procedure
Rev. 08	1/4/2016	Susan Heller-Zeisler	Added edits from Travel group
Rev. 09	3/1/2016	Susan Heller-Zeisler	Added AO edits
Rev. .10	5/3/2016	Susan Heller-Zeisler	Incorporated DRB Comments

Employment of Non-U.S. Citizens

NIST O 3112.00
Effective Date: 8/19/2013

PURPOSE

This Directive outlines requirements and responsibilities for employment of non-U.S. citizens and should be used in conjunction with the NIST PR 332 on the hiring of non-U.S. citizens. This document replaces Administrative Manual Subchapter 10.02.

APPLICABILITY

This Directive applies to the Federal employment of non-U.S. citizens at NIST.

LEGAL AUTHORITY AND REFERENCES

- 8 U.S.C. § 1324a (Unlawful employment of aliens);
- 15 U.S.C. § 278g (International activities);
- 5 C.F.R. § 213.3102(bb) (Entire executive civil service);
- 5 C.F.R. § 7.3 (Citizenship);
- 5 C.F.R. § 338.101 (Citizenship);
- 5 C.F.R. § 316.601 (Appointment without competitive examination in rare cases);
- 8 C.F.R. § 274a (Control of employment of aliens);
- Immigration Reform and Control Act of 1986;
- Immigration and Nationality Act of 1990;
- Consolidated Appropriations Act, 2012, Public Law 112-74;
- Executive Order 11935, dated September 2, 1976 (restricting the employment of non-citizens with limited exceptions);
- Department of Commerce (DOC) HR Bulletin #71, Hiring of Non-Citizens;
- NIST Directive PR 3112.01, Employment of Non-U.S. Citizens.

REQUIREMENTS

- NIST shall employ only U.S. citizens and persons owing permanent allegiance to the U.S., except when qualified citizens are not available.
- Per 15 U.S.C. § 278g, “National Institute of Standards and Technology, International Activities,” for any scientific and engineering disciplines for which there is a shortage of suitably qualified and available U.S. citizens and nationals, NIST may recruit and employ in scientific and engineering fields foreign nationals who have been lawfully admitted to

the U.S. for permanent residence under the Immigration and Nationality Act and who intend to become United States citizens.

- Per the Consolidated Appropriations Act, 2012, in relevant part, Unless otherwise specified in subsequent law, NIST may not use part of any appropriation to pay the compensation of any officer or employee whose post of duty is in the continental United States unless such person: (1) is a citizen of the United States; (2) is a person who is lawfully admitted for permanent residence and is seeking citizenship as outlined in 8 U.S.C. § 1324b(a)(3)(B); (3) is a person who is admitted as a refugee under 8 U.S.C. § 1157 or is granted asylum under 8 U.S.C. § 1158 and has filed a declaration of intention to become a lawful permanent resident and then a citizen when eligible; (4) is a person who owes allegiance to the United States; (5) is a person temporarily employed as a translator; (6) is a person temporarily employed in the field service (not to exceed 60 days) as a result of emergencies; or (7) is a person who was an officer or employee of the U.S. Government on December 23, 2011.
- NIST cannot employ non-U.S. citizens in positions that involve significant authority and responsibility in connection with NIST management, including, but not limited to, planning, policy formulation, direction, supervision of operations, and control.
- Prior to appointment, the Office of Workforce Management (OWM) will ensure that the DOC Office of Security conducts a risk assessment that considers the threat, consequences, and vulnerabilities related to employment of the non-U.S. citizen at NIST.
- Prior to hiring, the OWM will submit all non-U.S. citizen candidates for approval by the DOC Office of Human Resources Management (OHRM) and the Office of Personnel Management (OPM).
- OWM will appoint approved non-U.S. citizen hires to a Schedule A excepted appointment, authorized by 5 C.F.R. § 213.3102(bb).
- Hiring managers may not promote or reassign the non-U.S. citizen employee to another position in the competitive service, as the non-U.S. citizen does not acquire competitive status

RESPONSIBILITIES

International and Academic Affairs Office (IAAO)

- Oversees the visa requirements and immigration and naturalization regulations as they relate to NIST employees, associates and visitors.
- Determines the U.S. Citizenship and Immigration Services (USCIS) status viability for the prospective non-U.S. citizen appointee.

Department of Commerce (DOC) Office of Security (OSY)

- Conducts a risk assessment that considers the threat, consequences, and vulnerabilities related to employment of any non-U.S. citizen at NIST

Office of Workforce Management (OWM)

- Oversees the recruitment, hiring, and employment of non-U.S. citizens, primarily the appointment of non-U.S. citizens from the standpoint of the non-U.S. citizen's country of origin and the availability of any qualified U.S. citizens.

Department of Commerce, Office of Human Resources Management (OHRM) and Office of Personnel Management (OPM)

- Approves the appointment of the non-U.S. citizen.

U.S. Citizenship and Immigration Services (USCIS)

- Approves the visa request of the non-U.S. citizen.

DIRECTIVE OWNER

176 - Office of Workforce Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/7/2012	Dan Cipra	Initial Draft
Ver .01	10/24/12	Sandy Nail	Updates
Ver .02	4/5/13	Sandra Nail	Incorporated OCC and ELLD Changes.
Ver .03	4/16/13	Dan Cipra	Re-named to Non U.S. Citizens (global change), removed definition.
Ver .04	7/17/13	Dan Cipra	OCC, ELLD and DRB comments and changes accepted and incorporated.

Employment of Non-U.S. Citizens

NIST PR 3112.01
Effective Date: 08/19/2013

PURPOSE

This Directive outlines the procedures used in hiring non-U.S. citizens at NIST and should be used in conjunction with NIST Order O 332.01, Employment of Non-U.S. Citizens.

APPLICABILITY

This Directive applies to the employment of non-U.S. citizens at NIST.

LEGAL AUTHORITY AND REFERENCES

- 8 U.S.C. § 1324a (Unlawful employment of aliens);
- 15 U.S.C. § 278g (International Activities);
- 5 C.F.R. § 213.3102(bb) (Entire executive civil service);
- 5 C.F.R. § 7.3 (Citizenship);
- 5 C.F.R. § 338.101 (Citizenship);
- 5 C.F.R. § 316.601 (Appointment without competitive examination in rare cases);
- 8 C.F.R. § 274a (Control of employment of aliens);
- Immigration Reform and Control Act of 1986;
- Immigration and Nationality Act of 1990;
- Consolidated Appropriations Act, 2012, Public Law 112-74;
- Executive Order 11935, dated September 2, 1976 (restricting the employment of non-citizens with limited exceptions);
- Department of Commerce (DOC) HR Bulletin #71, Hiring of Non-Citizens;
- NIST Directive O 332 Employment of Non-U.S. Citizens.

PROCEDURES

NIST management may consider hiring a non-U.S. citizen candidate only when a qualified U.S. citizen is not available. The following steps outline the process for considering a non-U.S. citizen hire. If NIST is unable to successfully complete each phase of the process, the non-U.S. citizen may not be hired.

1. The hiring manager prepares a standard recruitment package along with a draft of the paid advertisement and submits it to the Office of Workforce Management (OWM). The OWM must review and approve all paid advertisements prior to posting.
 - a. A vacancy announcement must be posted for at least 30 days, and paid advertisements must appear in a minimum of two broad circulations such as local newspapers, professional journals, professional society circulars, bulletins, etc. The office is

responsible for ensuring that the paid advertisements are posted, following OWM approval, and for contacting subject matter experts in industry, academia, etc. (via letters, fax, e-mail) to request referral of any known qualified, interested U.S. citizens. Copies of any such correspondence should be forwarded to OWM for inclusion in the case file.

- b. Non-U.S. citizens may apply to the vacancy announcement but can only be considered for employment if no minimally qualified, interested U.S. citizens apply. All applicants (U.S. citizen and non-U.S. citizen) must submit the documentation required in the vacancy announcement.
2. If no U.S. citizen applies who is minimally qualified for the position and the hiring manager would like to hire a qualified non-U.S. citizen, the hiring manager prepares a justification memorandum regarding the proposed employment of the non-U.S. citizen. The memorandum must include the unique qualifications of the non-U.S. citizen, the benefit to the government if he or she is hired, and a detailed justification as to why other applicants were not found qualified. The memorandum is sent to the International and Academic Affairs Office (IAAO) through the Organizational Unit (OU) office. This memorandum must be approved by IAAO before moving forward with the remainder of the hiring process. Once it approves the memorandum, IAAO will send a copy of the memorandum to OWM.
 - a. Once the memo is approved by IAAO, the servicing Human Resources (HR) Specialist will require the non-U.S. citizen candidate to complete an OF-306, Declaration for Federal Employment. The HR Specialist will review the OF-306 for any suitability concerns and process it in accordance with the Pre-appointment Process Standard Operating Procedures, OSPD-2012-0009.
3. The Director, OWM, will submit a request to employ a non-U.S. citizen to the Director, Office of Human Resources Management (OHRM), Department of Commerce (DoC), for approval. The package must include:
 - SF-59, Request for Approval of Non-Competitive Action
 - Application of non-U.S. citizen candidate
 - Detailed justification of the qualifications of the non-U.S. citizen
 - Duties that will be performed (position description)
 - Security level of the position
 - Vacancy announcement
 - Outline of recruitment efforts and the results
 - Applications of all other candidates
 - Detailed justification of why all other applicants were not selected.
4. Once approved by OHRM, the request must be vetted and approved by the DoC Office of Security (OSY). The servicing HR Specialist will invite the non-U.S. citizen candidate into EQIP to complete an SF-85P, Questionnaire for Public Trust Positions. Fingerprint

arrangements will be made based upon the Pre-appointment Process Standard Operating Procedures, OSPD-2012-0009. To complete the review, the HR Specialist will obtain the following forms from the non-U.S. citizen candidate and, along with the completed OF-306, submit such forms to OSY:

- CD-79, Request for Security Clearance;¹
 - Job application;
 - Fair Credit Release; and
 - Declaration of Intent.
5. OWM will receive written clearance from OSY approving the hiring of the non-U.S. citizen candidate to the servicing HR Specialist. The servicing HR Specialist will then notify both OHRM and IAAO that OSY has provided the requisite clearance. OHRM will then submit the package to the Office of Personnel Management (OPM) for final approval. OPM certification can take one to two months to process. If OPM certification is not received, the non-U.S. citizen cannot be employed.
 6. Upon certification by OPM, if the non-U.S. citizen is in possession of a permanent resident visa, and intends to become a U.S. citizen, the background investigation is satisfactorily completed, and employment of the non-U.S. citizen is in compliance with the Consolidated Appropriations Act, 2012, or superseding law, and immigration laws, an offer of employment may be made by OWM.
 7. If the non-U.S. citizen is not in possession of a permanent resident visa, NIST must take additional steps to hire the individual.
 - a. If the non-U.S. citizen is not in possession of a permanent resident visa, NIST must file a petition on behalf of the non-U.S. citizen so that the individual may obtain the appropriate immigrant or nonimmigrant classification.
 - b. For a temporary worker, NIST must file a nonimmigrant petition on the non-U.S. citizen's behalf with U.S. Citizenship and Immigration Services (USCIS), Department of Homeland Security. The nonimmigrant petition appears in USCIS Form I-129, "Petition for a Nonimmigrant Worker."
 - c. For a permanent worker, NIST must file an immigrant petition on the non-U.S. citizen's behalf with USCIS. The immigrant petition appears in USCIS Form I-140, "Immigrant Petition for Alien Worker."
 - d. For some visa categories, prior to filing a petition with USCIS, NIST must also obtain an approved labor certification from the U.S. Department of Labor (DOL).

¹ The CD-79 must include the type of appointment; the position title, career path/pay plan, series, and pay band/grade; and the qualifications the non-citizen possesses that justify the appointment. The sensitivity level of the position must be low risk; the position may not have access to national security information or restricted areas; and the individual may not have policy-making responsibilities. The hiring office is charged the cost of the investigation whether or not the applicant is appointed. The investigation process may take approximately four to six months to complete.

- e. To obtain an approved labor certification, NIST must complete Department of Labor Employment and Training Administration (ETA) Form 9089, “Application for Permanent Employment Certification.” Initially, the hiring manager should complete Parts C, D and H of ETA Form 9089. Following completion of these Parts, the hiring manager provides ETA Form 9089 to OWM for further completion and review. Once OWM completes ETA Form 9089, it submits the application and all necessary paperwork to the U.S. Department of Labor. At the same time, OWM sends a copy of the completed ETA Form 9089, including all attachments, to IAAO. Approval from DOL may take several years.
 - f. After DOL provides an approved labor certification, NIST must submit an immigration petition to USCIS. Specifically, IAAO must complete USCIS Form I-140, “Immigrant Petition for Alien Worker.” IAAO then submits the DOL labor certification and the completed USCIS Form I-140 to the appropriate USCIS Service Center. The DOL labor certification has a validity period of 180 days and will expire if not submitted to USCIS within this period. The USCIS certification of Form I-140 can take up to several months. The USCIS website provides estimates on processing time.
 - g. After USCIS certifies the eligibility of the non-U.S. citizen to apply for permanent resident status and if a visa is available, the U.S. Department of State will notify NIST and the individual and invite the individual to apply for an immigrant visa. The non-U.S. citizen completes and files USCIS Form I-485, “Application to Register Permanent Residence or Adjust Status,” and submits it to USCIS. The individual must also apply for work authorization and an Employment Authorization Document (EAD) via [Form I-765](#), “Application for Employment Authorization.” The EAD serves as proof that the individual is allowed to work in the United States.
 - h. After USCIS approves employment authorization, and permanent resident status for the individual, NIST may make an offer of employment to the individual. The USCIS approval of permanent resident status can take one year or longer.
 - i. Where the non-citizen applicant is being considered for a job outside a scientific or engineering discipline and the applicant has been admitted as a refugee under 8 U.S.C. § 1157 or has been granted asylum under 8 U.S.C. § 1158 and has filed a declaration of intention to become a lawful permanent resident and then a citizen when eligible, once USCIS approves employment authorization, NIST may make an offer of employment to the individual.
 - j. Upon entrance on duty, non-U.S. citizen hires must complete the necessary enter-on-duty paperwork, including a USCIS Form I-9, “Employment Eligibility Verification.”
8. A non-U.S. citizen hired in the absence of a qualified citizen may only be given a Schedule A excepted appointment. In cases where OPM grants approval, the position must be withdrawn from the competitive service for the period it is filled by the non-U.S. citizen. The non-U.S. citizen employee does not acquire competitive status and may not be promoted or moved to other positions in the competitive service.

RECORD KEEPING

All relevant case file documents will be filed in the hiring management system.

DIRECTIVE OWNER

176 - Office of Workforce Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/11/2012	Dan Cipra	Initial Draft
Ver .01	10/25/12	Sandra Nail	Updates
Ver .02	4/5/13	Sandra Nail	OCC and ELLD Changes incorporated.

Merit Assignment Plan

NIST O 3113.00
Effective Date: 03/31/2014

PURPOSE

The Merit Assignment Plan (MAP) directive implements the Federal merit promotion and placement laws and regulations at the National Institute of Standards and Technology (NIST). Under the procedures established by this directive, qualified candidates have an opportunity to receive fair, equitable and appropriate consideration for promotion and placement to positions. In addition this directive describes the responsibilities of the Office of Human Resources Management (OHRM), Operations and Strategic Programs Division (OSPD); Selecting Officials; employees; and applicants.

APPLICABILITY

This directive applies to all competitive staffing actions involving status applicants. The following groups are also covered by this directive: (i) non-status applicants who are preference eligibles or veterans separated under honorable conditions from the armed forces after 3 or more years of continuous active military service; and (ii) applicants eligible based upon a special appointment authority. In some cases, the provisions of a collective bargaining agreement supersede this directive.

REFERENCES

- [Title 5, United States Code, Section 3304a](#), Competitive Service; career appointment after 3 years' temporary service
- [Title 5, United States Code, Section 2301\(b\)](#), Merit Assignment Plan
- [5 C.F.R. Part 335](#), Promotion and Internal Placement
- [Civil Service Reform Act of 1978](#)
- [Department Administrative Order \(DAO\) 202-335](#) Merit Assignment Program
- Federal Register Notices regarding the NIST Alternative Personnel Management System (APMS) (See Appendix A for a list of related notices)
- [Human Resources Bulletin #033](#), Job Analysis – Roles and Responsibilities
- [Human Resources Bulletin #119](#), Schedule A Appointing Authority for Persons with Disabilities
- [Human Resources Bulletin #144](#), Creating a Vacancy Announcement

REQUIREMENTS

- All employees and applicants for employment shall receive fair and equitable treatment in all aspects of human resources management without regard to political or labor

organization affiliation or non-affiliation, race, color, religion, national origin, sex, marital status, age, sexual orientation, or non-disqualifying disability, and with proper regard for their privacy and constitutional rights.

- This directive does not guarantee promotion but is intended to ensure that qualified applicants shall receive fair and equitable consideration for positions filled under competitive procedures.
- Supervisors may fill a vacancy by other appropriate sources, such as reemployment priority, reinstatement, transfer, special appointment authority (such as Schedule A or Veterans' Recruitment Appointment), or those within reach on an appropriate non-status certificate.
- Applicants may be considered concurrently or consecutively when using multiple recruitment sources.
- Subject to laws and regulations, Selecting Officials shall make the final decision on candidate selections and have the right to select or not select from among the best-qualified candidates.
- HR Specialists have delegated authority to approve final personnel actions for Merit Assignment Plan appointments.
- Selecting Officials have delegated authority to approve final pay for new appointees or employee promotions.

DEFINITIONS

Ability – The power to perform an observable activity at the present time.

Area of Consideration - The area of consideration defines the scope or source from which applications will be accepted. The area of consideration is set forth in the vacancy announcement in the section titled "Who May Apply." Sources include status applicants (i.e., current Federal permanent employees and former Federal employees with reinstatement rights) and applicants eligible for special appointment authorities (e.g., Veterans' Recruitment Appointment (VRA), 30% Disabled Veterans, Veterans Employment Opportunity Act (VEOA), Peace Corps volunteers, Individuals with Disability, Career Transition Assistance Plan (CTAP) and/or Interagency Career Transition Assistance Plan (ICTAP) eligibles).

Best Qualified - A designator for those qualified applicants who rank the highest when compared with other qualified applicants and are referred to Selecting Officials for hiring consideration.

Certificate – A list of eligibles from which a Selecting Officer selects for appointment.

MAP Certificate – The document used to refer the best-qualified competitive status applicants to a Selecting Official and to document selection or non-selection.

Noncompetitive Certificate – The document used to refer to a Selecting Official qualified applicants eligible for selection under special appointment authorities and to document selection or non-selection.

Detail - The temporary assignment of an employee to a different position or set of duties for a specified period of time with no change in pay.

Job Analysis - A systematic procedure for gathering, documenting, and analyzing information about the content, context, and requirements of the job. It demonstrates that there is a clear relationship between the tasks performed on the job and the competencies/Knowledge, Skills and Abilities (KSAs) required to perform those tasks, and results in a valid crediting plan.

Job Elements - Knowledge, skills, abilities, or other characteristics essential for performance in a Federal Wage System position.

Knowledge - An organized body of information, usually of a factual or procedural nature, resulting from education or training.

Known Promotion Potential (KPP) - The highest grade or pay band of a position (also called the Full Performance Level (FPL)).

Merit Assignment Program Vacancy Announcement – The document used to publicize vacancies under this directive and to inform potential applicants about the position being filled, its qualification requirements, the information required to be submitted, and the procedures to follow to receive consideration.

Non-Status Applicants – Applicants who are not currently employed in the Federal service or do not have reinstatement rights based on former Federal service.

Pay Band - A level of classification within a career path under the NIST APMS classification program. (Replaces grades under General Schedule (GS) classification system.).

Priority Consideration - The referral of an individual to a Selecting Official in advance of other qualified applicants for selection consideration. Eligibility for priority consideration is based on provisions of law, regulation, court order, or settlement.

Promotion -

Promotion for NIST APMS Employees Only - The change of an employee to: (a) a higher pay band in the same career path; or (b) a pay band in another career path in combination with an increase in pay. The minimum pay increase upon promotion is six percent of salary or the amount required to reach the minimum of the new band if that amount is greater than six percent. In the latter instance, the maximum pay increase is limited to the cap of the new pay band.

Promotion for GS Employees - The change of an employee, while continuously employed, to a higher grade level.

Promotion for Federal Wage System (FWS) Employees - The change of an employee, while continuously employed, to a higher FWS grade in the same type of prevailing wage schedule

Accretion of Duties Promotion - The noncompetitive promotion beyond the career ladder/KPP to a higher grade, pay band in the same career path, or higher FWS grade because the position has been reclassified due to additional higher-level duties and responsibilities.

Career Promotion - The noncompetitive promotion of an employee to a pay band/grade for which the employee previously competed.

Quality Ranking Factor (QRF) – A job-related knowledge, skill, and/or ability that is desirable or expected to significantly enhance performance in a position. QRF's are the basis for determining an applicant's rank in comparison to other qualified applicants.

Rating - A numerical score indicating the degree to which an applicant possesses the job-related knowledge, skills and abilities, outlined by quality ranking factors or job elements of the position.

Reassignment -

Competitive - The change of an employee, while serving continuously within the same agency, from one position to another position at the same band or grade level but with greater promotion potential.

Non-Competitive - The change of an employee, while serving continuously within the same agency, from one position to another position with no increase in pay and no greater promotion potential, promotion, or demotion. This action may be the result of the introduction of a new or revised classification or job grading standard or position review.

Skill - The proficient manual, verbal, or mental manipulation of data or things.

Screen Out Element - A critical element that establishes the minimum qualifications required for an FWS position. Applicants who do not meet the lowest acceptable requirement in the screen-out element are deemed unqualified for the position.

Selective Factor - A job-related knowledge, skill, and/or ability that is required for satisfactory performance in a position. A selective factor is in addition to the basic OPM qualification standard for a position and is therefore part of the minimum qualification requirements that applicants for the position must meet to be minimally qualified.

Specialized Experience - Experience that has equipped the applicant with the particular knowledge, skills, and abilities to perform successfully the duties of the position and where the skills are typical for or related to the work of the position to be filled.

Status Applicants - Those applicants who are employed currently in the Federal service or who have reinstatement rights based on former Federal service.

Subject Matter Expert (SME) - An individual who has full knowledge of the duties of the position and the knowledge, skills, and abilities necessary to perform the work of the position. SME must be in the same grade level or higher than the position to be filled. The SME cannot be the hiring official or an applicant for the position. The SME must be a Federal employee, not a contractor.

Transfer - The change of an employee as a result of a vacancy from a position in one agency to a position in another agency.

RESPONSIBILITIES

Operations and Strategic Programs Division (OSPD)

- Establish, implement and administer this directive.
- Advise and train supervisors and employees on the requirements, objectives, and other aspects of this directive.
- Establish and maintain necessary files on each selection sufficient to permit reconstruction of personnel actions and to answer inquiries.
- Advise on the area of consideration.
- Publish the vacancy announcement and advise Selecting Officials on the development of the job analysis, hiring tools, special hiring authority options, the description of specialized experience, selective factor(s), screen-out element(s), quality ranking factor(s), job element(s), and assessment criteria.
- Evaluate the minimum qualifications of applicants and/or advise panel members of their responsibility in making this determination.
- Prepare the MAP and noncompetitive certificates.
- Approve requests for MAP certificate extensions.
- Make the official position offer.
- Ensure that priority placement programs are applied.
- As requested, serve on merit assignment panel evaluations in an advisory capacity as a non-voting member.
- Periodically offer training on this directive.

Selecting Officials

- Staff positions in accordance with applicable Federal laws and regulations.
- Develop position descriptions, compile information for vacancy announcements, and develop the job analysis to include:
 - The description of specialized experience;
 - Selective factor(s);
 - Screen-out element(s);
 - Quality ranking factor(s);
 - Job element(s); and
 - Assessment criteria.

- Determine the area of consideration that will produce an adequate number of best-qualified and diverse applicants.
- Identify the appropriate Subject Matter Expert (SME) who has full knowledge of the duties of the position, the skills and abilities necessary to perform the work and who will be responsible for providing relevant information related to the position.
- Adhere to merit system principles and select from among the best-qualified applicants.

Applicants

- Comply with requirements stated in the vacancy announcement.
- Meet all eligibility requirements by the closing date of a vacancy announcement.
- Ensure that their applications are complete, timely, and submitted in accordance with the instructions contained in the vacancy announcement prior to the vacancy closing date.

SMEs

- Review the applicants against the minimum qualification requirements.
- Provide the servicing Human Resources (HR) Specialist with a list of qualified candidates (by grade level) and a list of unqualified candidates (with justification).
- If applicable, provide a justification when changing applicant self-assessment responses. The justification should identify where in the resume or cover letter the applicant either demonstrates they have (or do not have) experience, indicate which applicant assessment response should be changed, and specify how the response should be revised.
- Immediately notify the servicing HR Specialist if there is a nepotism issue, a supervisory relationship, or a close professional or personal relationship to the applicant that could influence the qualification analysis
- Consider only relevant information provided in the application, including the resume and cover letter

CONSIDERATION AND SELECTION OF QUALIFIED APPLICANTS

Coverage:

- A. Subject to the exceptions listed in subsection (B) below, the competitive procedures of this directive apply to the following actions:
 1. Promotion actions;
 2. Selection for training when training is required for promotion or part of an authorized training agreement or promotion plan;

3. Reassignment, demotion, transfer, or reinstatement to a position with greater promotion potential in the competitive service;
 4. Reassignment to at a higher pay band/grade than previously held on a permanent basis in the competitive service;
 5. Temporary promotion for over 120 days;
 6. Details for more than 120 days to a position at a higher pay band/grade or with greater known promotion potential; and
 7. Any combination of (5) and (6) where the total service would exceed 120 days during the previous 12 month period.
- B. Exceptions: The competitive procedures of this directive do not apply to the following actions:
1. A promotion resulting from upgrading a position, without a significant change in the duties and responsibilities, due to the issuance of a new classification standard or the correction of an initial classification error;
 2. A position change permitted by reduction-in-force procedures;
 3. The upgrading of an employee's position due to accretion of additional higher pay band/grade duties and responsibilities when the successor position absorbs the major duties of the former position;
 4. A career promotion when an employee was selected previously under competitive procedures for a position below the full performance level;
 5. Non-competitive conversion from the Student Pathways Program, Presidential Management Fellow Program, and other authorized programs;
 6. Promotion from a trainee position when the employee was selected for the target position under competitive procedures;
 7. Temporary promotion or detail to a higher pay band/grade for 120 calendar days or less (all details to higher pay band/grade positions and temporary promotions held during the preceding 12-month period are counted when computing the 120-day period);
 8. Promotion, reassignment, demotion, transfer, reinstatement, or detail provided: (i) the position to be filled is at no higher grade than that previously held on a permanent basis under a career or career conditional appointment; (ii) the position has no known promotion potential (KPP) beyond that of the employee's current position or the potential is not more than the highest grade previously held; and (iii) the employee was not demoted or separated from that grade because of deficiencies in performance or other "for cause" reasons;
 9. Promotion of a candidate who was not given proper consideration in a competitive promotion action;

10. An increase in pay due to supervisory differential;
11. Selection under direct hire, agency-based staffing, or delegated examining authorities;
12. Selection from Department of Commerce Reemployment priority list (RPL); and
13. Voluntary change to a lower grade with no greater KPP than position last held.

Area of Consideration

- A. The area of consideration must be sufficiently broad to ensure the availability of an adequate number of best-qualified and diverse applicants for the Selecting Official's consideration. The area of consideration must adhere to current NIST and Department of Commerce (DOC) policies.
- B. A status applicant may request to be considered as both an internal and an external applicant; consideration will be in accordance with the applicant decision for each vacancy announced.
- C. Employees within the area of consideration who are absent for legitimate reasons (e.g., on detail, on leave, at training courses, in the military service, or serving in public international organizations or on Intergovernmental Personnel Act assignments) must receive proper consideration for promotion.

Vacancy Announcement

Under this directive, a vacancy announcement must remain open for a period consistent with current DOC policy.

Qualification and Evaluation:

- A. The job analysis will serve as the basis for determining the qualification requirements based upon the position duties and responsibilities. The job analysis must be conducted in a manner consistent with current DOC policy and procedure. Additionally, the NIST HR website for Documents Required for Personnel Actions provides a job analysis sample template.
 1. Qualification Standards for General Schedule Positions, published by OPM, are used to determine basic eligibility of applicants. All applicants must meet the qualification requirements for the position by the closing date of the announcement. For APMS positions, the qualification standard for the lowest grade in the pay band is used to determine basic eligibility.
 2. The job elements used to qualify for FWS positions are contained in the Office of Personnel Management (OPM) Handbook X-118C, Job Qualification System for Trades and Labor Occupations.
- B. Prior to posting the position on USAJOBS, the Hiring Manager must notify the servicing HR Specialist if an SME will conduct qualification analysis. SME review is not required.

Referral and Selection:

- A. Pursuant to DAO 202-335, priority consideration will be given to employees who have been involuntarily downgraded (for other than cause) for at least a minimum of two years after their demotion in both their current operating unit and the operating unit where their demotion occurred. Additionally, priority consideration/referral will be given to qualified individuals who meet all eligibility criteria for the CTAP, ICTAP, or the RPL. Selection must be in the following order:
1. NIST/National Technical Information Service (NTIS) CTAP;
 2. NIST/NTIS Employees (i.e., internal reassignments, promotions, and voluntary change to lower grade);
 3. DOC CTAP – Local commuting area;
 4. DOC CTAP – Outside of the local commuting area;
 5. Status DOC Employees;
 6. RPL Candidates;
 7. ICTAP – Local commuting area;
 8. Status Federal employees; and
 9. Non-status applicants
- B. The MAP Certificate will list the names of the best-qualified competitive candidates for the vacancy to be filled. NIST defines best-qualified competitive candidates as candidates that receive an overall score in the “Gold” range.
- C. In addition to the highly qualified candidates referred on the MAP Certificate, qualified candidates may be referred on Noncompetitive Certificates as follows:
1. Qualified Merit candidates that previously competed for or held the highest grade/band level of the position being advertised can be referred on a Noncompetitive Certificate. If selected, current Federal service employees will be reassigned or transferred into the position with no increase in pay.
 2. Best-qualified candidates eligible for special appointment authorities may also be referred under a Noncompetitive Certificate. The most common special appointment authorities are: Schedule A (individuals with disability), VRA, and 30% Disabled Veterans.
- D. Selecting Officials may request that additional names be added to a MAP Certificate if applicants on the original certificate decline or withdraw from further consideration, fail to reply, or are removed from consideration by the Selecting Official, provided the Selecting Official can justify in writing why the referred applicant is not suitable for selection. The number of additional names added to the Certificate should not exceed the number of applicants removed from the original Certificate. Selecting Officials may request additional applications when applicants have been removed from consideration and the Selecting

Official can justify in writing why the referred applicants are not suitable for selection to the position.

- E. The vacancy may be re-posted immediately if there are fewer than three qualified applicants to be referred on the MAP Certificate.
- F. The MAP Certificate is issued to the Selecting Official and is only valid for 30 calendar days from the date issued. The MAP Certificate may be extended only with the approval of the Chief, OSPD, based upon a written justification from the Selecting Official. Each request should state the amount of time necessary to complete the selection decision and the basis for this determination, keeping in mind the President's hiring reform agenda and the "Pledge to Applicants." A request to extend a certificate for more than an additional 30 days will require the Selecting Official to obtain the OU Director's concurrence prior to submission of the request.
- G. The Selecting Official may select any of the referred candidates on the MAP Certificate or Noncompetitive Certificate.
- H. Selecting Officials must give performance appraisals and incentive awards due weight in the selection process and prior to making the selection decision (e.g., during interviews or when conducting reference checks).
- I. Selecting Officials may interview any number of the applicants referred. Interviews may be conducted by telephone where face-to-face interviews are not possible.
- J. Interview panel members must be at the same grade level or higher than the position to be filled.
- K. The Selecting Official is not required to fill a vacancy by selection from a MAP Certificate. Other appropriate sources may be used such as: Direct Hire/Delegated Examining Authority, Agency Based Authority, noncompetitive reassignment, reinstatement, transfer, special appointing authorities, VRA, and others.
- L. The Selecting Official's decision to select an applicant is subject to all other approvals required by law, regulation, or policy.
- M. The Selecting Official shall indicate the tentative selection decision and other actions as required on the MAP Certificate. The signed certificate must indicate the disposition of each applicant and be returned to OSPD along with the signed certification page indicating completion of the Management Satisfaction Survey no later than the certificate's expiration date. No final offer of employment may be made until the OSPD staff determines that all required approvals and clearances have been obtained. The HR Specialist will make the final job offer, notify the Selecting Official of the selectee's decision, and confirm the effective date of the action.
- N. The OSPD arranges the Entrance-on-Duty (EOD) date. If the selectee is a current NIST employee and is being reassigned, NIST requires that the selectee be released from current organization or agency within two pay periods. If the selectee is a current NIST employee

and is being promoted to a higher grade or pay band, NIST requires that the selectee be released from current organization at the beginning of the first pay period after selected. Under unusual circumstances, the release period may be extended by mutual agreement.

- O. Applicants have the right to review records used to evaluate them under this directive in accordance with applicable Privacy Act and Freedom of Information Act regulations. Records are maintained for two years or until after an OPM audit, whichever is sooner.
- P. Applicants may request, in writing to the Chief, OSPD, reconsideration of the qualifications determination made by the HR Specialist. The request must explain why the original determination was improper; what factors were not considered; and, should provide any other pertinent information that would enable the Chief, OSPD to reevaluate the decision. Applicants determined to have “lost consideration” will receive consideration for the next vacancy in the same career path, series, pay band for which qualified.

CAREER LADDERS/KNOWN PROMOTION POTENTIAL (KPP):

Career ladders/KPP are the successive grades/pay bands through which an employee may advance to the full performance level within an occupation or group of like occupations. Incumbents may be promoted noncompetitively upon demonstration of their ability and readiness to perform at the next higher pay band or grade in the career ladder, and when legal requirements are met. No employee shall receive a career ladder promotion unless the employee’s current rating of record is “Fully Successful” (level 3) for Wage Grade or GS, or Contributor for APMS, or higher. In addition, no employee may receive a career ladder promotion if the employee has a rating below “Fully Successful” (level 3) for Wage Grade or GS, on a critical element that is also crucial to successfully performing at the next higher grade of the career ladder.

The NIST designated career ladders/KPP include:

- All Scientific and Engineering (ZP) positions to Pay Band III;
- All Scientific and Engineering Technician (ZT) positions to Pay Band II;
- All Administrative (ZA) positions to Pay Band III;
- The following Support (ZS) positions:
 - 0081, Firefighter – IV;
 - 0203, HR Assistant – IV;
 - 0303, Administrative Support Assistant – IV;
 - 0318, Secretary;
 - Group Level Secretaries – III;
 - Division/Office, OU Deputy Director, SMA Level Secretaries – IV;
 - OU Director and Above– V;

0525, Accounting Technician – IV; and

- The following GS positions:

0083, Police Officer - 07;

- Wage Grade Positions. Career ladder/KPP of each position is determined individually and stated on the vacancy announcement.

Exceptions to the above career ladders require written documentation as to the reasons for the limitation. This documentation will be filed in the vacancy case file.

DIRECTIVE OWNER

175 – OHRM, Operations and Strategic Programs Division (OSPD)

APPENDIX

- A.** Federal Register Notices regarding the NIST Alternative Personnel Management System (APMS)
- B.** Revision History

APPENDIX A

FEDERAL REGISTER NOTICES REGARDING THE NIST ALTERNATIVE PERSONNEL MANAGEMENT SYSTEM (APMS)

52 Fed. Reg. 37082 (Oct. 2, 1987)
54 Fed. Reg. 21331 (May 17, 1989)
54 Fed. Reg. 33790 (Aug. 16, 1989)
55 Fed. Reg. 19688 (May 10, 1990)
55 Fed. Reg. 39220 (Sept. 25, 1990)
52 Fed. Reg. 54604 (Oct. 21, 1997)
70 Fed. Reg. 23996 (May 6, 2005)
73 Fed. Reg. 40500 (July 15, 2008)
74 Fed. Reg. 35841 (July 21, 2009)
74 Fed. Reg. 35843 (July 21, 2009)
76 Fed. Reg. 539 (Jan. 5, 2011)
76 Fed. Reg. 78889 (Dec. 20, 2011)
77 Fed. Reg. 36485 (June 19, 2012)
77 Fed. Reg. 48128 (Aug. 13, 2012)
77 Fed. Reg. 51518 (Aug. 24, 2012)

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	6/8/2012	Dan Cipra	Initial Draft
Ver .01	3/1/2013	Sandra Nail	Change in referral of candidates to include Noncompetitive Certificate procedures for candidates that previously held or competed for the higher grade.
Ver .02	7/5/2013	Sandra Nail	Updated based on OCC Comments
Ver .03	12/12/2013	Dan Cipra	Created clean copy based on OGC and OCC changes.
Ver. .04	1/28/2014	Dan Cipra	Updated based on DRB comments.
Ver. .05	2/18/2014	Sandra Nail	Updated comment from ELLD.
Ver. .06	3/27/2014	Dan Cipra	Created a clean copy with updated comments.
Rev. .07	2/3/2016	Dan Cipra	Updated Directive Number and related information.

Associate Entrance on Duty and Separation Clearance

NIST O 3114.00
Effective Date: 1/13/2010

PURPOSE

This directive establishes the requirements and responsibilities necessary for the National Institute of Standards and Technology (NIST) Associate entrance on duty and separation processing and supports the coordination and completion of tasks using the required worksheets and the NIST Associate Information System (NAIS–Web).

APPLICABILITY

This directive applies to the arrival and departure of all NIST Associates of all types at NIST Gaithersburg and NIST Boulder. This directive does not apply to visitors

REFERENCES

- [5 U.S. Code 3371 – 3376](#)
- [15 U.S. Code 272\(b\)\(4\), \(c\)\(7\)](#)
- [15 U.S. Code 278g\(a\)](#)
- [15 U.S. Code 278g-1](#)
- [15 U.S. Code 278g-2](#)
- [15 U.S. Code 3710a](#)
- [15 C.F.R. 334.103-334.108](#)
- [Department of Commerce DAO 207-1 Security Programs](#)
- [Department of Commerce DAO 201-11 Official Credentials and Badges](#)
- [Department of Commerce DAO 207-12 Foreign National Visitor and Guest Access Program](#)
- [P 3100.00 Human Resources Management](#) (6/26/2014)

DEFINITIONS

NIST Associate – Any non-employee who is a U.S. citizen, comes to a NIST campus and/or uses NIST information technology (IT) resources, and is either working in a lab (for any period of time) or on campus for more than ten working days. Click for the [NIST Associate Listing](#).

Contracting Officer's Technical Representative (COTR) – The Federal employee assigned to represent a NIST Contracting Officer when developing requirements for task orders affiliated with NIST Associate contracted work. The COTR is the individual responsible for accepting deliverables within each statement of work.

Emergency Services Division (ESD) – Office responsible for registration and issuance of NIST site badges.

Foreign National Associate – Any NIST Associate that is not a U.S. Citizen, including permanent residents.

NIST Associate Information System (NAIS) - Web – The web-based application that automates the preparation, review, and approval of all NIST Associate agreements, records, extensions, and security forms. NAIS-Web provides the ability to retrieve data using reports and is an integral part of completing the NIST Associate Entrance on Duty Worksheet and NIST Associate Separation Clearance Worksheet.

NAIS Host – The Federal employee administratively supporting the NIST Associate. It is recommended that the COTR fill this role for Associates working at NIST on a contract.

NAIS Initiator – The individual within the Organizational Unit (OU) or Division who originates NIST Associate forms in NAIS, including Guest Researcher Agreements and security forms.

PIV Sponsor – A Federal employee who has been approved by the NIST Role Administrator, Emergency Services Division (ESD) upon completion of the U.S. Access PIV Sponsor Training.

REQUIREMENTS

- The NIST Associate Entrance on Duty Worksheet and the NIST Associate Separation Clearance Worksheet shall be used to manage and organize the NIST Associate's pre-arrival and post-arrival processes, as well as to ensure that separation clearance tasks are completed as required. To find the appropriate required worksheet document, visit the [NAIS Templates web page](#).
- For new NIST Associates, all tasks outlined in the NIST Associate Entrance on Duty Worksheet must be completed unless they are determined by an appropriate NIST official not to be applicable. Prior to separation, all tasks listed in the NIST Associate Separation Clearance Worksheet must be completed, unless they are not applicable. Tasks on the first page of the NIST Associate Separation Clearance Worksheet should be completed before an Associate concludes his or her tenure at NIST, and in the case of tasks

identified for completion on "Last Day" must be completed before an Associate concludes his or her tenure at NIST.

- The worksheets identify necessary steps and requirements associated with tasks that are essential to ensuring that NIST Associates experience a smooth on-board and separation process. The worksheets are relevant to individuals with assigned roles related to coordinating the completion of these tasks. Worksheets should be followed as completely as possible. Note, however, that some tasks may not be applicable in certain circumstances, in which case non-applicable entries should be labeled with "N/A" and initialed and dated.
- Worksheets must be retained for a period of at least one year after the Associate is no longer at NIST.

RESPONSIBILITIES

Individuals in the roles identified below shall complete the relevant tasks based on the timing requirements specified. These will often be the Associate's NAIS Host or NAIS Initiator, but NIST Operating Units and Chief Offices may make local determinations regarding who are the most appropriate individuals to serve in these roles and carry out these tasks.

OU Directors and Division Chiefs:

- Review and approve or disapprove Associate agreements. Division Chiefs shall ensure that this policy is followed by all with a role in implementing it.

Office of Security (OSY):

- Perform the personal security investigation

Technology Partnerships Office (TPO):

- Assist with questions regarding arrival and departure of Domestic Associates, particularly Domestic Guest Researchers

International and Academic Affairs Office (IAAO):

- Assists with questions regarding arrival and departure of Foreign National Associates, particularly Foreign Guest Researchers.

Onboarding Office (OB):

- Ensures that NIST Associates receive the proper orientation and training needed to safely and securely perform their function at NIST.
- Provide a consistent set of training and orientation to all NAs including safety, physical security and operational security, and information technology security.

Division Administrative Officer:

- Files/retains Worksheets for a period of at least one year after the Associate is no longer at NIST.

Group leaders, Team Leads or equivalent roles:

- Manage the review process for Associates in some OUs.

NIST Initiators:

- Assists those individuals accountable for completing tasks outlined in each worksheet.

NIST Associates:

- Perform the steps necessary for completing the NIST Associate Entrance on Duty Worksheet and NIST Associate Separation Clearance Worksheet.

NIST Hosts and COTRs:

- Verify completion of the NIST Associate Entrance on Duty Worksheet and NIST Associate Separation Clearance Worksheet
- File the worksheets upon completion.

Worksheet Owner:

- Ensures that tasks on the worksheets are carried out in a timely fashion, and that worksheets have been submitted to the Division Administrative Officer for retention.
- The role of Worksheet Owner may be assigned to an individual who already has another role identified on the worksheets (e.g., a NAIS Host or NAIS Initiator may also serve as the Worksheet Owner).

DIRECTIVE OWNER

190 – Chief Facilities Management Officer

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	2 Feb 10	Janet Hoffman (OHRM)	First Draft
Rev. .01	3 Feb 16	Dan Cipra (M&O)	Formatting Updates Only

Separation Clearance

NIST O 3115.00
Effective Date: 9/12/2009

PURPOSE

This directive defines the responsibilities for NIST employees to clear their accountability for property, records, funds, and other matters when NIST employees separate from NIST.

APPLICABILITY

This directive is applicable to all NIST Employees.

REFERENCE

- Department of Commerce [Department Administrative Order \(DAO\) 202-299](#)

DEFINITIONS

Terminal Leave - Leave taken immediately before separation or retirement and after the employee has performed his or her last day of active duty. Leave under these circumstances is prohibited.

RESPONSIBILITIES

Employee

- Shall follow supervisory instructions and the NIST clearance procedures. The employee must obtain clearance from every office function listed on Forms [CD-126](#), Separation Clearance Certificate and [NIST-598](#), Separation Clearance Certificate (Supplemental Sheet to CD-126), prior to supervisory certification of the forms. Once the forms are complete, the employee must return them to his or her supervisor, who will complete Section IV on Form CD-126, sign as appropriate on Form NIST-598, and forward the forms to the servicing Human Resources Office. The employee's final salary payment, lump-sum payment, and any other payments will not be processed and issued until these forms are completed and cleared in their entirety.
- Each separating employee is encouraged to complete the NIST Exit Survey. The NIST Exit Survey can be completed online at the web address provided on the form NIST-598. The purpose of this survey is to learn what motivates people to leave NIST, to obtain constructive suggestions for improvement of policies and practices, and to ascertain opinions on morale, operations, and other factors. Survey responses are anonymous and are entered into a database from which statistical summaries and trend data are produced and used to drive improvements at NIST.

- The employee should contact the Human Resources Office or the Civil Rights and Diversity Office if the employee wants to have an Exit Interview with an HR Specialist or an EEO Counselor.
- As a general rule, the date of separation must be the last day worked when separating from Federal service. A supervisor may not grant an employee terminal leave immediately prior to separation from Federal service when it is known in advance that the employee is to be separated, except where the exigencies of the service require such action.

Clearance Officials

- Shall approve the clearance of chargeable items by printing in and signing the applicable block with his/her full name, date and telephone number or by having an administrative staff enter the clearance officials name, date and telephone number. If applicable, clearance officials must note the reason any chargeable item is not accounted for or returned, and if appropriate, indicate the dollar value of the unaccounted item(s) to be collected from the employee. Clearance officials must follow the clearance procedures to ensure designated authorizing official(s) have cleared.

Supervisor

- In accordance with Department and operating unit guidance, the separating employee's immediate supervisor is responsible for:
 1. Initiating Forms CD-126, Separation Clearance Certificate and NIST-598, Separation Clearance Certificate (Supplemental Sheet to CD-126), one week prior to an employee's separation date;
 2. Completing Section I of Form CD-126, advising the employee of the employee's responsibilities regarding the clearance process, and providing the forms to the employee;
 3. Upon the employee's receipt of all clearance signatures and the employee's completion of Section III, Employee Certification, completing Section IV, Supervisor Certification, and submitting the completed forms to the Human Resources Office; and
 4. Certifying the final time and attendance (T&A) record (if applicable) only if the employee has properly obtained clearance, in accordance with Forms CD-126 and NIST-598. If the employee has not properly obtained clearance, the Supervisor can withhold the final salary payment by not certifying the "final" T&A.

Servicing HR Office

- The servicing HR Office is responsible for acknowledging receipt of Forms CD-126 and NIST-598 and indicating whether or not each form was completed in its entirety. If a form is not complete, the HR Office will return the form to the supervisor or take the necessary steps to collect the debt. Final salary payment, lump sum payment, or any other payments may not be released until the debt is resolved. "Debts" can include unpaid travel charges, library fines, negative leave balances, NFC bills that have yet to be collected, etc.

- Forms CD-126, Separation Clearance Certificate and NIST-598, Separation Clearance Certificate (Supplemental Sheet to CD-126), must be completed in their entirety and certified with the supervisor's signature. If any items on the forms are not applicable, they should be marked as such. Accordingly, every item on the forms should have a response. If any items are left unmarked, the form will be returned to the supervisor for completion. Any item not cleared by the clearance official can result in the employee's final salary payment being withheld until a settlement is made. The supervisor or clearance official should inform the employee and contact the servicing HR Specialist of any items not cleared. This gives the HR Office notice to withhold the employee's last salary payment and/or lump sum payment or make arrangements for settlement prior to the employee's separation date.

DIRECTIVE OWNER

190 - Office of Workforce Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	10/17/2011	OHRM POC	Initial Draft – Grandfathered from Admin Manual
Rev. .01	10/23/2011	Dan Cipra	Formatting updates only

Disciplinary/Adverse Actions

NIST O 3120.00
Effective Date: 9/13/2016

PURPOSE

This directive sets forth specific requirements and responsibilities for the National Institute of Standards and Technology (NIST) when addressing employee misconduct via discipline and other appropriate corrective actions.

APPLICABILITY

This order applies to NIST employees except where in conflict with provisions of an applicable [collective bargaining agreement](#).

REFERENCES

- [Title 5, United States Code, Chapters 73 and 75](#) Adverse Actions
- [Title 5, Code of Federal Regulations \(CFR\), Part 752](#), Adverse Actions
- [Title 5, CFR 731](#), Suitability
- [Title 5, CFR 735](#), Employee Responsibilities and Conduct
- [Title 5, CFR 315](#), Career and Career-Conditional Employment
- [Title 5, CFR 534](#), Pay Under Other Systems
- [Title 5, CFR 2635](#), Standards of Ethical Conduct for Employees of the Executive Branch
- [Departmental Administrative Order \(DAO\) 202-751](#), Discipline
- [DAO 202-771](#), Administrative Grievance Procedure
- [DAO 202-955](#), Allegations of Harassment Prohibited by Federal Law
- [DAO 207-10](#), Inspector General Investigations
- [Department of Commerce, Human Resources Bulletin, Domestic Violence Policy](#), January 3, 2014
- [Department of Commerce, Human Resources Bulletin, Addressing Workplace Violence Policy](#), May 14, 2014
- [P 3100.00](#) Human Resources Management

DEFINITIONS

Alternative Discipline - Alternative discipline is an action taken to correct an employee's behavior other than using the traditional disciplinary methods under DAO 202-751. It involves the employee, the employee's representative (if applicable), and the supervisor reaching a voluntary agreement with the goal to correct an employee's improper behavior and accomplishes the objectives of both parties.

Day(s) – Calendar day(s) unless otherwise noted in the action taken.

Delegation of Authority – The authority given to appropriate management officials within an Organizational Unit (OU) to take appropriate action (e.g., propose or decide) against an employee for misconduct.

Proposing Official – A management official who proposes a disciplinary or adverse action (e.g. a proposed suspension, demotion or removal from Federal service). This individual is usually in an employee's supervisory chain.

Deciding Official – A management official who makes a decision regarding a proposal to suspend, demote, or remove an employee from Federal service. This individual is usually in an employee's supervisory chain and is usually one administrative or organizational level above the proposing official.

Removal - An involuntary separation from the Federal service. A Standard Form (SF) 50 documenting the removal from Federal service will be placed on the permanent side of the employee's Official Personnel Folder (OPF).

Reprimand – A written notice from a supervisor to an employee addressing unacceptable conduct, stating what must be done to improve and warning that failure to correct the problem may result in more serious action by the supervisor. The written reprimand is placed in the employee's OPF a minimum period of one (1) year up to a maximum period of three (3) years. The supervisor has the discretion to remove the reprimand from the employee's OPF at any point during this time period. Once the reprimand is removed from the OPF, it can no longer be used to enhance the penalty for subsequent misconduct, i.e., referenced as a prior disciplinary action. However, it may be used or referenced in subsequent action to demonstrate that the employee received notice of expectations of proper conduct.

Suspension – Involuntary placement of an employee in a non-duty status without pay or work for disciplinary reasons. A Standard Form (SF) 50 documenting the suspension will be placed on the permanent side of the employee's OPF.

REQUIREMENTS

- A management official or supervisor who is considering taking an action under this order shall consult with OHRM to ensure that the action being considered is appropriate.
- Action taken to address misconduct administered under this order shall promote the efficiency of the Federal service and be accomplished in a timely, constructive, and consistent manner. Although progressive discipline should generally be considered, NIST

recognizes that some employee misconduct may warrant more severe action, including removal for a first offense.

- Action taken to address employee misconduct shall comply with this order, NIST policies and procedures, DoC guidance and Federal regulations and laws. Consideration should be given to the recommendations in the DoC Table of Offenses and Penalties.”
- Alternative discipline will be used, where appropriate.
- Each OU will identify management officials who are delegated the authority to take actions under this order. Each OU shall communicate such delegation to OHRM.
- The NIST Director may be both the proposing and deciding official.
- When a supervisor has a reasonable belief that an employee’s unacceptable conduct may be caused in whole or in part by personal problems, including but not limited to family issues or substance abuse, the supervisor should suggest that the employee seek assistance through the NIST Employee Assistance Program (EAP).
- The decision to terminate a probationary, trial or temporary employee or re-employed annuitant must be made at least one level above the first-level supervisor.

RESPONSIBILITIES

Organizational Unit (OU) Director

- Delegates the authority to take action under this order.
- Sets OU-wide standards regarding employee workplace expectations.
- Ensures that management addresses misconduct in a timely and effective manner.

Office of Human Resources Management (OHRM) Director

- Educates and/or informs employees of relevant Federal laws, regulations, and DoC and NIST policies and procedures.
- Advises supervisors and managers on appropriate action to be taken in individual cases.
- Reviews and ensures that disciplinary and adverse actions conform with Federal laws and regulations, and DoC and NIST policies, and follow sound personnel practices.
- Consults with the DoC Office of General Counsel (OGC) regarding issues of law, consistent with DAO 202-751.
- Informs employees who are involved in actions under this order of their rights.
- Retains official case records for actions taken under this order in accordance with NIST Comprehensive Records Schedule.

Department of Commerce, Office of General Counsel (OGC)

- Provides legal advice and guidance consistent with law, rule and regulation (e.g., DAO 202-751).

Supervisor or designated management official

- Sets and enforces the workplace expectations; assigns work.
- Addresses workplace misconduct and deficiencies as they occur so as to correct the employee's behavior. When such actions do not result in employee conformance, takes timely appropriate action utilizing this order. Such action may include serving as a proposing or deciding official on any actions under this order based on the OU's delegation of authority.
- Maintains documentation in support of actions covered under this order.
- Seeks OHRM advice when addressing employee matters (to ensure technical requirements of the law and regulations have been met).

Employees

- Learn about and comply with Federal laws, rules, regulations, and DOC and NIST policies governing behavior and conduct of NIST/Federal employees.
- Conduct themselves, on and off duty, in a manner consistent with Federal laws, rules, and regulations and DOC and NIST policies concerning behavior, and in a way which reflects well on themselves, NIST, and the federal workforce.
- If an employee believes that an action is taken against them improperly, he or she may seek redress, as applicable, through venues such as the NIST Equal Employment Opportunity complaint process, Merit Systems Protection Board appeal process, DoC's administrative grievance procedure, and/or grievance under a negotiated grievance procedure. Generally, employees may utilize only one path of redress.

DIRECTIVE OWNER

0176 - Office of Human Resources Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	7/8/2016	Micha Bratten	Initial Draft
Rev. .01	8/2/2016	Dan Cipra	Formatting

Incentive Awards

NIST O 3123.00
Effective Date: 7/6/2016

PURPOSE

The purpose of this directive is to provide NIST specific requirements, responsibilities, and authorities regarding the utilization of incentive awards.

APPLICABILITY

This directive applies to all NIST employees.

LEGAL AUTHORITIES & REFERENCES

- [Title 5, United States Code, \(U.S.C.\), Chapter 43, Performance Appraisal](#)
- [Title 5, U.S.C., Government Organization and Employees, Chapter 45, Incentive Awards §4501 to §4523](#)
- [Title 5, Code of Federal Regulations \(C.F.R.\), §430, Performance Management](#)
- [Title 5, C.F.R., §451, Awards](#)
- [DAO 202-430: Performance Management System](#)
- [The Recognition Section of the Performance Management System Handbook](#)
- Alternative Personnel Management System: [National Technical Transfer and Advancement Act of 1995](#), Public Law 104-113, §10 (1996)
- [P 3100.00](#) Human Resources Management

DEFINITIONS

Awards - Something bestowed or an action taken to recognize and reward individual or team achievement that contributes to meeting organizational goals or improving the efficiency, effectiveness, and economy of the Government or is otherwise in the public interest as defined by [Title 5 CFR §451.102, Definitions, Awards](#).

Bronze Medal - The highest honorary award granted by a head of DOC operating unit or Secretarial Officer or equivalent. A Bronze Medal is defined as superior performance characterized by outstanding or significant contributions, which have increased the efficiency and effectiveness of the operating unit.

Cash-In-Your-Account - A monetary award which recognizes accomplishments representing steps toward achievement of organizational goals or purposes, but for which higher level recognition such as honor awards, performance awards, or special act awards are not

appropriate. Awards may be granted for noteworthy contributions benefiting the individual's employing office, bureau, or the Department.

Colleagues' Choice Award Review Panel - The Colleagues' Choice Award Review Panel acts as an advisory body, which reviews nominations and makes recommendations on recipients to the NIST Director for an award that recognizes non-supervisory employees of NIST who, in the eyes of their colleagues, have made significant contributions that broadly advance the NIST mission and strategic goals or broadly contribute to the overall health and effectiveness of NIST.

Department of Commerce Honor Awards - The DOC's highest form of honorary recognition that is granted to DOC employees. The awards include Gold, Silver, and Bronze Medals.

NIST Editorial Review Board (ERB) - The ERB acts as an advisory body, which reviews the Condon nominations, a NIST Award, and makes recommendations on recipients to the NIST Director for an award that recognizes and promotes distinguished achievement in written exposition in science or technology published by NIST employees.

External Awards - Awards sponsored through external award programs that have specific guidance announced by the sponsors annually and which are distributed through the NIST Office of Human Resources Management.

Gold Medal - The highest honorary award granted by the DOC Secretary. A Gold Medal is defined as distinguished performance characterized by extraordinary, notable, or prestigious contributions that impact the mission of the Department and/or one or more operating units, which reflects favorably on the Department unit (DOC Performance Management Handbook, Chapter 10).

Incentive Awards Program - The specific procedures and requirements established by NIST for granting awards under subchapter I of Chapter 43 and subchapter I of Chapter 45 of Title 5, United States Code of subpart 451.102.

NIST Awards - Annual awards that are awarded to NIST employees based on the criteria for each named award. The eligibility and criteria for each award are located on the Awards page.

NIST Incentive Awards Panel (NIAP) - The NIAP membership consists of representatives from the Director's Office, Management Resources, Innovation and Industry Services, and Laboratory Programs Directorates. The NIAP acts as an advisory body, which reviews nominations and makes recommendations on recipients of Honor and NIST Awards, as well as external awards requiring the NIST Director's approval.

On-the-Spot Awards - Recognize accomplishments that represent steps toward achievement of organizational goals or purposes, for which higher-level recognition such as honor awards, performance awards, or superior accomplishment awards are not appropriate. The eligibility requirements and criteria are located on the Awards page.

[Peer-to-Peer Awards](#) - A small monetary award initiated by NIST employees to recognize the contributions of their peers and co-workers. The eligibility requirements and criteria are located on the [Awards](#) page.

[Presidential Rank Awards](#) - Presidential Rank Awards recognize career Senior Executive Service (SES) members for exceptional performance over an extended period of time and senior career employees with a sustained record of exceptional professional, technical, and/or scientific achievement recognized on a national or international level.

[Special Act Award](#) - A monetary award given in recognition of an employee achievement or contribution or as payment as an incentive. The eligibility requirements and criteria are located on the [Awards](#) page.

[Silver Medal](#) - The second highest honorary award granted by the DOC Secretary. A Silver Medal is defined as exceptional performance characterized by noteworthy or superlative contributions, which have a direct and lasting impact within the Department.

[Time-Off as an Incentive Award](#) - An award given to an employee or group of employees in the form of paid time off in recognition of superior accomplishment or personal effort that contributes to the quality, efficiency, or economy of Federal Government operations. The eligibility requirements and criteria are located on the [Awards](#) page.

REQUIREMENTS

- The guidelines in the Department of Commerce's (DOC) Performance Management System Handbook must be adhered to.
- The Gold and Silver medals nominations will adhere to the [awards cycle](#) specified by the Department.
- The NIST Awards and Bronze medals nominations will adhere to the [awards cycle](#) specified by the NIST Director.
- An employee must meet the [eligibility requirements](#) for the award for which he/she is nominated.
- The Cash-In-Your-Account, On-the-Spot, Peer-to-Peer, Special Act, and Time Off nominations are accepted on an ongoing basis.
- All Cash-In-Your-Account, On-the-Spot, Peer-to-Peer, Special Act, and Time-Off nominations must be completed in their entirety on a Recommendation for Recognition form ([CD-326](#)).
- All Gold and Silver nominations must be completed in their entirety on the [Gold/Silver nomination form](#).
- All Bronze nominations must be completed in their entirety on the [Bronze nomination form](#).
- All NIST Awards nominations must be completed in their entirety on the appropriate NIST Awards [nomination form](#).

ROLES AND RESPONSIBILITIES

NIST Director

- Annually requests nominations for the DOC Honor Awards and the NIST Awards;
- Recommends the following awards:
 - Gold and Silver Honor Medal Awards;
 - Presidential Rank Awards;
 - External Awards for NIST nominees; and
 - SES/SL/ST Special Act Awards.
- Approves the following awards:
 - NIST Awards;
 - Bronze Honor Medal Awards; and
 - Direct subordinate's nominations.

Associate Directors and Organizational Unit Directors, and Office Directors, Division Chiefs

- Recommend the following awards:
 - Special Act Awards;
 - External Awards for NIST nominees;
 - DOC Honor Awards; and
 - NIST Awards.
- Approve direct subordinate's nominations for the following awards:
 - Special Act Awards (excluding SES/SL/ST);
 - Cash-In-Your Account Awards;
 - On-the-Spot Awards; and
 - Time-Off Awards.

Division Chief

- Additionally, approves nominations for Peer-to-Peer Awards.

First Level Supervisor

- Recommend nominations for the following awards:
 - Special Act Awards;
 - Cash-In-Your-Account Awards;
 - On-the-Spot Awards;

- Time-Off Awards;
- External Awards for NIST nominees;
- DOC Honor Awards; and
- NIST Awards.

NIST Employees

- Recommend employees for the following awards:
 - Peer-to-Peer Awards; and
 - Colleagues Choice Award.

NIST Office of Human Resources Management

- Plans, coordinates, and administers the incentive awards program under the general policy guidance of the NIST Director;
- Audits and evaluates the incentive awards program for effectiveness; and
- Retains all incentive awards records in accordance with the [NIST Records Schedule item 66](#).

NIST Incentive Awards Panel ([NIAP](#))

- Reviews and evaluates nominations for the following awards:
 - Gold, Silver, and Bronze Medals;
 - NIST Awards (except Condon, Safety and Colleague's Choice awards); and
 - Any other awards at the request of the NIST Director;
- Discusses and makes award recommendations on the aforementioned awards via the prescribed voting and meeting procedures;
- Develops sub-panels to review specific awards requiring certain expertise; and
- Recommends procedural changes in the NIAP process.

NIST Chief Safety Officer

- Reviews and evaluates all of the Safety Award nominations using the specific criteria listed under NIST Awards on the [Awards](#) page; and
- Recommends nominations to the NIST Director for approval.

Editorial Review Board ([ERB](#))

- Reviews and evaluates all of the Edward Uhler Condon Award nominations using the specific criteria listed on the [Awards](#) page; and
- Recommends nominees to the NIST Director for approval.

Colleagues' Choice Award Review Panel

- Reviews and evaluates all of the Colleagues' Choice Award nominations using the specific criteria listed on the [Awards](#) page; and
- Recommends nominees to the NIST Director for approval.

DIRECTIVE OWNER

Office of Human Resources Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	4/19/2016	Morgan Frycklund	Initial Draft
Rev. .01	4/20/2016	Dan Cipra	Formatting updates
Rev. .02	6/2/2016	Morgan Frycklund	Incorporated DRB Comments

Zero Tolerance Harassment Policy

NIST P 3200.00
Effective Date: 4/16/2013

PURPOSE

To ensure that NIST provides its employees with a work environment that is free from unlawful harassment.

SCOPE

This policy applies to all NIST employees.

LEGAL AUTHORITIES

- Title VII of the Civil Rights Act of 1964, as amended;
- The Age Discrimination in Employment Act of 1967;
- The Rehabilitation Act of 1973;
- Executive Order 11478 (as amended by EO 12106 and further amended by EO 13087);
and
- Department Administrative Order (DAO) 202-955.

POLICY

The Department of Commerce and NIST do not tolerate discrimination or harassment based on race, color, religion, sex (including sexual harassment and pregnancy discrimination), sexual orientation, gender identity, national origin, age (40 years of age and over), genetic information or disability (physical or mental), including the provision of reasonable accommodations for qualified applicants and employees with disabilities. Retaliation against those who initiate discrimination complaints, serve as witnesses, or otherwise oppose discrimination and harassment is also strictly prohibited.

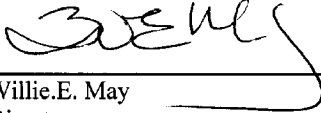
Even in the absence of a tangible job action, treating someone differently because of one of these protected characteristics can rise to the level of unlawful harassment through the creation of a hostile work environment if the behavior is: directed at a person because of a protected characteristic; unwanted; and sufficiently severe or pervasive so as to interfere with the terms or conditions of a person's employment. Harassment is a form of discrimination that can include unwelcome, unsolicited, persistent, pervasive, verbal or non-verbal, and/or physical conduct that has the purpose or effect of creating or contributing to an intimidating, hostile, or offensive work environment; unreasonably interfering with work performance; or negatively affecting employment opportunities. Harassment tends to be an offense of a repetitive nature although one

incident may constitute harassment if sufficiently serious. Activities that could be considered harassment may include, but are not limited to, derogatory or suggestive comments which are offensive in nature and disruptive and counterproductive to the NIST work environment. Slurs, gestures, and offensive posters, cartoons, pictures, and or drawings may be offensive and determined to be a form of harassment.

All NIST employees are strongly encouraged to report any incident they perceive to be prohibited harassment, to include incidents personally experienced and those witnessed. They may either report it to their immediate supervisor, a higher level supervisor or to the NIST Director of the Office of Human Resources Management (OHRM) as soon as the incident occurs.

NIST managers and supervisors must immediately report any and all alleged, suspected, or perceived harassment, in writing, to the NIST OHRM Director. Failure by the manager or supervisor to comply with this reporting requirement could result in disciplinary or adverse action against the manager or supervisor for failure to adhere to the provisions of this policy. A manager or supervisor who receives any allegation of harassment, or perceives or suspects harassment, against an employee must inform the employee of his or her right to seek counseling from the NIST Civil Rights & Diversity Office (CRDO). The employee should be informed that all counseling contacts must occur within 45 days from the date of the alleged harassing event.

Any NIST employee found to have engaged in harassment will be subject to disciplinary action up to and including removal from the Federal service.



Willie.E. May
Director

2/04/16
Date

Identification of Institutional Support Rate Type

NIST PR 4000.01

Effective Date: 8/13/2013

Last update: 10/2/2015

PURPOSE

The purpose of this directive is to define the various rate types used by NIST to collect Institutional Support (IS) funds based on all NIST obligations (this includes all object classes).

APPLICABILITY

This directive applies to all NIST obligations.

REFERENCES

- Office of Financial Resource Management (OFRM) Resource Center Budget Surcharge Rates https://iwebd2.nist.gov:4445/ofrm_dev/NIST_Budget/Budget_Surcharge.html
- NIST Administrative Manual Subchapter 8.05, *NIST Work Performed for Others* (8/8/2012)

DEFINITIONS:

All NIST obligations – All funds that NIST obligates for direct costs in the current fiscal year. This includes undelivered orders and accruals in the current fund code fiscal year for all object classes.

Double taxation – Twofold assessment of an IS rate on the same direct costs.

Earmark – Funds provided by the Congress for projects or programs where the congressional direction circumvents the competitive allocation processes, or specifies the location or recipient, or otherwise curtails the ability of NIST to manage critical aspects of the funds allocation process.

Exempt – Excluded from an IS assessment.

Extramural obligations – Funding awarded by NIST via grant or cooperative agreement.

Flat rate – An assessment against obligations (direct costs) at a fixed percentage to cover indirect costs.

Institutional Support – Funding collected via fixed percentage rates against obligations of NIST resources to fund costs associated with general administration and centralized services as defined by NIST.

Intramural obligations – Total obligations for direct costs less extramural obligations.

Lite rate – An assessment against obligations at a fixed percentage lower than the flat rate to cover indirect costs.

Majority – Greater than 50 percent.

Off-Site – A non-NIST site.

Off-Site rate – An assessment against obligations at a fixed percentage to cover only appropriate indirect costs for work being performed by NIST employees at off-site locations. (See Off site Rate Checklist for [STRS](#) and [Reimbursable](#) Funding)

Override – An annually approved request by a program for a change to the rate type from that indicated in the decision tree.

Program – All funding, both appropriated and reimbursable, assigned to a specific program code related to an Organizational Unit (OU).

Reimbursable obligations – External funds that NIST receives via reimbursable agreement (e.g., interagency agreements, memoranda of agreement/understanding and obligates to perform work for others in Fund Code 08.

Split rate – A combination of the flat and lite rates.

REQUIREMENTS

1. The appropriate IS rate will be applied to all NIST obligations.
2. The percentage assessed for each rate type will be published by the Budget Division on the OFRM Resource Center Budget Surcharge Rate page.
3. All NIST resources will be charged the rate type determined by the *Institutional Support Rate Decision Tree (see chart)* unless an approved *NIST-609 – Institutional Support Rate Type Override Request (Appendix A)*, approved by the NIST Director, is on file with the Budget Division.
4. For each of the IS-rate types identified: Flat rate, Lite rate, Off-Site rate, and Split rate, the collections will occur monthly (month end) via system generated cost allocation templates.

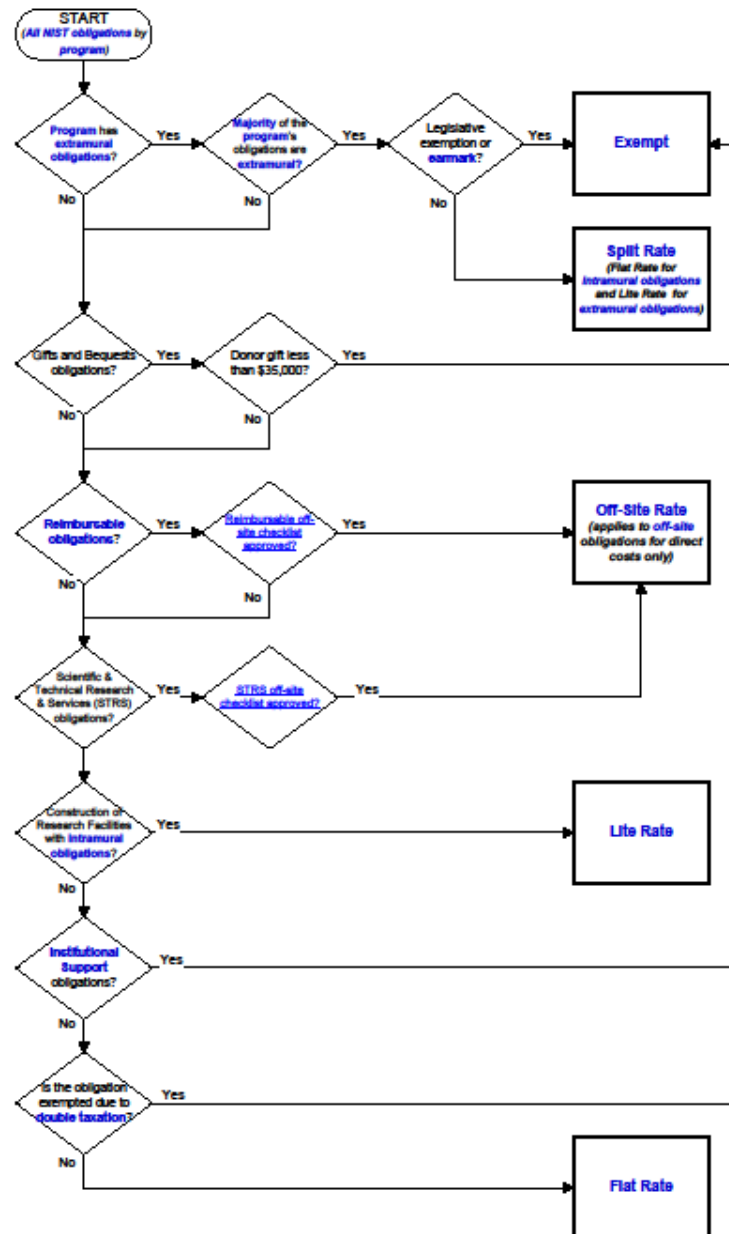
PROCEDURES

Identification of Institutional Support Rate Type:

The Institutional Support rate type to be assessed is identified by the IS Rate Type Decision Tree:

Institutional Support Rate Type Decision Tree

10/2/2015



Requesting a Rate Type Override:

On no less than a fiscal year basis, a program may request an override of the rate type determined by the *Institutional Support Rate Decision Tree* (see chart) by completing *NIST-609 – Institutional Support Rate-Type Override Request* (Appendix A). The form must be approved by the appropriate OU Director and submitted to the Budget Division for review and recommendation. NIST Senior Management will review the request and either approve or disapprove. The program will be notified of the decision within 15 business days of its submission. The override is only effective for the fiscal year for which it is requested and approved.

Rate-type changes will be applied at the beginning of the fiscal year after approval is obtained. Approved rate-type overrides must be on file with the Budget Division by June 30 of the previous fiscal year in order to be applied at the beginning of the next fiscal year.

New Programs:

A new program will have 15 business days, from the receipt of the allocation, to request override status. The process of requesting a rate-type override proceeds as described above once the request is received. Override approval for a new program must be on file with the Budget Division within 30 business days from the receipt of the allocation.

***Note:** A rate-type override request may be submitted for a new program prior to the receipt of the official allocation.*

Initial Implementation:

For the initial implementation of this directive in FY 2013, all existing programs will be treated as new programs to establish rate types going forward.

DIRECTIVE OWNER

160 – OFRM

APPENDIX:

Terms in **blue** text are defined in the Definitions section of this document.

Type Override Request

B. Revision History

A. NIST-609 –
Institutional
Support Rate-

APPENDIX A

NIST-609– INSTITUTIONAL SUPPORT RATE-TYPE OVERRIDE REQUEST

NIST-609
(7-2012)
NIST PR 506.01

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

IS RATE TYPE OVERRIDE REQUEST

REQUESTOR NAME: REQUEST DATE:

PROGRAM NAME:

PROGRAM CODE:

PROJECT TYPE:

PROJECT CODE(S):

ORIGINAL RATE TYPE: ☐ Exempt ☐ Lite Rate ☐ Off-Site Rate ☐ Split Rate ☐ Flat Rate

OVERRIDE RATE TYPE: ☐ Exempt ☐ Lite Rate ☐ Off-Site Rate ☐ Split Rate ☐ Flat Rate

EFFECTIVE DATES FOR OVERRIDE:
From: To:

REASON FOR OVERRIDE:

OU DIRECTOR APPROVAL:

TITLE	Approve	Disapprove	SIGNATURE	DATE
Director, OU	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

BUDGET DIVISION REVIEW:

TITLE	Approve	Disapprove	SIGNATURE	DATE
Budget Officer, Budget Division	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

NIST SENIOR MANGEMENT REVIEW:

TITLE	RECOMMENDATION		SIGNATURE	DATE
	Approve	Disapprove		
Associate Director, Laboratory Programs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Associate Director, Innovation and Industry Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Associate Director, Management Resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

APPROVAL/DISAPPROVAL:

TITLE	Approve	Disapprove	SIGNATURE	DATE
Director, NIST	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

COMMENTS:

Reset Form

Print Form

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Ver. 4.0	10/1/2015	Amber Hunter Terri Working Diane Holland	Updated Decision Tree to include STRS off-site approval and link to checklist.
Ver. 3.0	1/26/2015	Amber Hunter Terri Working Diane Holland Cyndi Greathouse	Removed “SCMMR” from Definition section (page 2). Deleted IS Rate type, collection method and frequency table because they are all now processed the same via the system. (page 2) Revised decision tree removing the SCMMR diamond based on the signed memo from Acting NIST Director 1.9.15 (page 3)
Ver. 2.0	7/17/2013	Amber Hunter Terri Working Diane Holland	Added “SCMMR” to the Definitions section (page 2). Revised decision tree in the Procedures section (page 3) to address SCMMR funding based on the override implemented in FY 2013.
Ver. 1.4	8/17/2012	Amber Hunter Terri Working Diane Holland	Incorporated, where appropriate, recommendations from the DRB meeting on 8/17/12.
Ver. 1.3	8/15/2012	Amber Hunter Terri Working Diane Holland	Incorporated, where appropriate, recommendations from the DRB.
Ver. 1.2	8/9/2012	Katie Schlatter	Incorporated recommendations from Legal and updated document with final form name, number and image.
Ver. 1.1	7/26/2012	Dan Cipra	Format update
	7/25/2012	Katie Schlatter	Initial Draft

Working Capital Fund

NIST PR 4100.01

Effective Date: 2/25/2016

PURPOSE

This directive establishes the procedures for the National Institute of Standards and Technology (NIST) Working Capital Fund (WCF). These include the distribution of indirect charges to projects as overhead; the management of expense and income (E&I) projects; the purchase and/or manufacture of invested equipment (IE) and associated loan repayments; the production of Standard Reference Materials (SRMs); and SRM and storeroom inventories.

APPLICABILITY

This directive applies to all of NIST.

At Boulder, the NOAA Corporate Finance and Administrative Services Office provides storeroom services for NIST and other participating agencies.

REFERENCES

- [Public Law 81-583 \(64 STAT. 275\)](#) which established the Working Capital Fund authorized NIST to use the Fund for expenses and operations and to collect reimbursements from applicable appropriations and other agencies for facilities and services provided. Reimbursements were to include handling and related charges, reserves for depreciation of equipment and accrued leave, and building construction and alterations directly related to work for which the reimbursement was made.
- [15 USC 278b](#) authorized NIST to credit the Fund with advances and reimbursements, including receipts from non-federal sources.
- [Public Law 99-73](#) in 1985 authorized the WCF to retain earnings to ensure the availability of funds to replace equipment and inventories.

PROCEDURES

Working Capital Fund (WCF) - general

- 1) The WCF is a revolving fund that finances all NIST indirect costs and is reimbursed from NIST appropriations and reimbursable sources. Through a detailed cost accounting system, the actual cost of work performed for each task is recorded and identified with the appropriate source of financing.
- 2) In addition to its function as a revolving fund, the WCF permits the handling of annual leave on an accrued cost basis, the acquisition of equipment as an investment to be recovered through Invested Equipment (IE) loan repayments, the distribution of indirect

charges to projects as overhead, the production of Standard Reference Materials (SRMs), and the holding of SRM and storeroom inventories.

- 3) The amount of available capital in the WCF consists of the original appropriated capital, Congressionally-approved transfers from NIST appropriations, and replacement surcharges (see NIST Administrative Manual Subchapter 8.08 Cost Accounting).

Reimbursements to the WCF in excess of costs are recorded as earned net income or profits to the WCF. Profits or losses may arise from charging fixed prices for certain services and from applying certain costs on a rate basis. At the end of each fiscal year, the amount of any earned net income resulting from the operation of the Fund is to be paid into the general fund of the U.S. Treasury, provided that such earned net income may be applied first to restore any prior impairment of the fund and to ensure the availability of working capital necessary to replace equipment and inventories. (15 US Code (U.S.C.) 278b (f)). Similarly losses should be factored into subsequent pricings and/or rates to address any impairment and ensure the working capital is fully restored.

Leave and Benefits

The Deficiency Appropriation Act of 1950 that established the WCF directed NIST to maintain reserves for accrued leave. As leave is earned by employees, it is funded by the Organizational Units (OUs) via a rate charged against labor costs. The cost and the liability for leave earned is recorded in the WCF. This liability must be adjusted as Federal employees enter and leave NIST employment and as pay rates change. The Finance Division monitors the liability and adjusts the rate as necessary to maintain the correct reserve balance. When leave is used, the employee is paid from the leave reserve in the WCF. The Government's share of employee benefit costs are also funded via a rate applied to labor and leave costs and are paid from the WCF. The benefits rate is monitored by the Finance Division and adjusted as necessary to cover costs.

Institutional Support

1) Most Federal agencies receive a direct appropriation for the cost of general administration, program direction, staff services and other similar costs. A separate appropriation for these functions is not provided to NIST; therefore, such costs must be distributed as a charge to all projects not funded by Institutional Support (IS) as determined by the [IS Rate Type Decision Tree](#) within [NIST PR 4001.01](#) Identification of Institutional Support Rate Type.

There are three different IS rate types used to collect funds to reimburse the WCF:

- Flat Rate – An assessment against obligations (direct costs of labor and other objects) at a fixed percentage to cover indirect costs.
- Lite Rate – An assessment against obligations at a fixed percentage lower than the flat rate to cover indirect costs. Typically these would include extramural contracts or grants.

- Off-Site Rate – An assessment against obligations at a fixed percentage to cover only appropriate indirect costs for work being performed by NIST employees at off-site locations. Work must meet all the criteria on the Off-Site rate check lists for STRS or Reimbursable funding.

2) Separate projects are established in IS-funded organizations to record the costs of the four major categories of IS activities which include:

- i. General administration and staff services, including assessments from the Department of Commerce, executive direction, financial management, human resources management, management and organization functions, basic information technology services and NIST-wide infrastructure, grants and agreements management, acquisition management, and other NIST-wide services such as mail distribution, safety and security programs, storeroom management, and transportation management.
- ii. Operation and maintenance of facilities, including janitorial services and physical security, plant maintenance, utilities, and telephone services.
- iii. Technical support, including occupational health and safety, administrative and business systems support, and library services.
- iv. Activities where operating efficiency, practicality, or equality are gained by centralizing the activity.

3) NIST management decides which activities shall be funded through IS. IS functions are reviewed periodically to ensure that they are financed by the most efficient and equitable method. Some criteria applied in this review are:

- i. Operating Efficiency - Is there a management advantage to using IS versus direct charging for the services? In some cases, there is a more efficient use of resources if costs are charged directly to projects; however, in other cases, central financing and management achieve greater efficiency.
- ii. Practicality - What is the most practical and inexpensive way to identify the customer and record the appropriate cost?
- iii. Equality - Does the cost distribution mechanism place the costs where they belong? A service may be centrally provided to support technical programs, but, unless its use is widely dispersed, charging through IS produces not only unrealistic but also inequitable charges.

4) Where feasible, NIST permits the IS budget to grow in proportion to the appropriations and/or reimbursable funding on which it is assessed. So for example, if appropriated and reimbursable funding is flat in a given year, then NIST management may determine that the IS budget will be flat as well and the IS rate will remain unchanged. This should mitigate unanticipated rate increases. Certain expenses which are dictated by external circumstances, such as utilities, are designated as "uncontrollable" and, by definition, are authorized at the

level required to cover the cost. The Federal budget appropriation process offers the following mechanisms for securing funding and increasing staff for IS areas:

- i. Adjustments to Base (ATB) are calculated to include the appropriation's share of inflationary increases in IS costs.
- ii. Initiative pricings are calculated to include the impact of the larger technical program on IS services and other expanded IS needs.

5) Determination of IS authorization levels for the coming year is a multi-stage process.

- i. Each spring, the Budget Division develops and issues initial total estimated allocation levels to each IS-funded organization. These levels may reflect adjustments such as salary-annualizations for approved prior year initiatives and other ATBs.
- ii. In late summer, IS-funded organizations prepare and submit detailed budget reviews and initiative requests for increases over the annual allocation level. The IS-funded organizations present the initiatives to the Associate Director for Management Resources (ADMR) and Budget Division staff.
- iii. The ADMR evaluates the initiatives, discusses with other NIST Management (Director, Chief of Staff and Associate Directors), and initial decisions are determined.

6) IS allocations are summarized at the IS-funded organization level. Monthly “operating budgets” are distributed by the Budget Division to track the allocations distributed during the year. The ADMR must be consulted before any action is taken which requires the commitment of additional IS funds.

7) All IS costs are paid directly from the WCF, and the WCF is reimbursed through several mechanisms see NIST PR 4001.01 (link: <http://inet.nist.gov/ofrm/directives/identification-of-is-rate-type.cfm>)

8) IS Project Types - The following project types are to be used for IS-funded activities (See also NIST Administrative Manual Subchapter 8.02 Fund Structure Appendices A and B):

- IOHBAS - base labor and other objects that continue on an annual basis and are managed by the IS organization,
- IOHOUR - IS organization non-base one-time distribution made within their organization using base funding,
- IOHDIR - ADMR non-base from the NIST IS reserve funds and are generally unique in nature and have a short term funding requirement, and
- IOHUNC – Uncontrollable costs that recur but fluctuate in price due to external conditions such as utilities.

IS projects operate on an obligation basis where total obligations must be covered via IS collections.

Laboratory Overhead

- 1) Laboratory Overhead Costs - Laboratory overhead projects accumulate the costs of developing, managing, and coordinating the overall program of the laboratory. Costs properly chargeable to laboratory overhead may include:
 - i. Salaries, leave, personnel benefits and the applicable overhead surcharges, and performance bonuses for laboratory office staff, the laboratory director, the laboratory deputy director, division chiefs, executive officer, senior management advisor, administrative officers and assistants, and secretaries; and other positions offering laboratory-wide support.
 - ii. Other objects essential to effective laboratory office operations, including supplies, materials, travel, and special laboratory-wide program studies.
 - iii. Selected training costs of employees attending broad program training at the request of the laboratory director. Specialized training identifiable with programs within a division should not be charged to laboratory overhead.
 - iv. Moving or reorganization costs resulting from the move of several offices or an entire division ordered by the laboratory director to consolidate operations, to provide space for new programs, or to improve overall laboratory efficiency.
 - v. IE loan repayments.
- 2) Some costs are not properly chargeable to laboratory overhead. Examples include:
 - i. Costs which can be identified with a specific program.
 - ii. Technical activities normally financed by direct appropriations or reimbursements.
 - iii. Start-up or termination costs associated with technical programs.
- 3) Distribution of Cost - Laboratory overhead costs are offset by collections from benefiting projects using rates which are applied to labor, leave, benefits and other objects, charged to laboratory projects each month.

The laboratory has the option of handling IE loan repayments either centrally or on a division basis, as described below.

Option I: A single laboratory rate is set to collect funds to cover all overhead costs, including IE loan repayments.

This option consolidates and monitors IE loan repayments at the laboratory level and is used if the distribution of the IE loan repayments at the laboratory level is determined to be equitable. Monthly charges are made against the designated laboratory overhead projects in the OHLAB project type (series 910-919). Thus, all benefiting projects throughout the laboratory will fund a share of the IE loan repayments.

Option II: A laboratory rate is set to collect funds to cover overhead costs at the laboratory level; this rate may include collections for IE loan repayments charged to OHLAB projects only (series 910-919); and

Separate division overhead rates are set to collect funds to cover the IE loan repayments charged to OHDIVE projects (series 900-909).

Option II should be used when separate monitoring of IE loan repayments is required at the division level to ensure equitable financing. (Example Division 1 uses IE funding of \$500K to purchase equipment that will only benefit Division 1. Division 2 uses IE funding of \$25K to purchase equipment that will only benefit Division 2. Therefore it is more equitable for each division to have a separate division rate.)

Prior to the start of the fiscal year, each OU must determine if its current Laboratory Overhead option is still appropriate. If a change is necessary, a memorandum is transmitted to the Finance Division, with a copy to the Budget Division, stating the Laboratory Overhead option selected. The memorandum should be submitted at the same time that Laboratory Overhead Plans are submitted to the Budget Division.

- 4) Laboratory Overhead Project Series - The following project numbering series is recommended for Laboratory Overhead projects (see [NIST Administrative Manual Subchapter 8.02 Fund Structure Appendixes A and B](#)):
 - OHLAB Laboratory Overhead Expense (Options I and II) 910-919 (ex. 7700910)
 - OHDIVE Division IE Loan Repayment Overhead Expense (Option II only) 900-909 (ex. 7700900)
- 5) Laboratory Overhead projects operate on an obligation accounting basis where current-year obligations and prior year adjustments must be covered by current year collections.
- 6) Establishing the Laboratory/Division Overhead Rate - [Form NIST-627](#), Notification of Predetermined Overhead Rate, is used to establish or change a laboratory overhead or a division IE loan repayment overhead rate. [Form NIST-627](#) is prepared and approved in the OU, submitted to the Budget Division for review, and entered into the accounting system by the Finance Division. NIST Administrative Manual Subchapter 8.08 Cost Accounting, Appendix D, contains the procedure for establishing predetermined overhead rates via [Form NIST-627](#).
- 7) Adjustments for Prior-Year Local Overhead Profits or Losses - The net end-of-fiscal-year profit or loss associated with each OU's overhead account(s) (laboratory and division) must be carried forward into the next fiscal year, noting that under certain circumstances these profits may need to be paid to the U.S. Treasury if it is determined the NIST WCF as a whole has made a profit. In addition, the OU's overhead collections in the new fiscal year will be adjusted via [Form NIST-627](#) to include the credit or debit received from the prior fiscal year's profit or loss.
- 8) Monitoring Spending - Each Laboratory and Division Overhead rate should be calculated by the OU to result in collections equal to the total estimated costs. It is the responsibility of each OU to review the accuracy of its overhead rate(s) and to revise the rate(s), as necessary, to prevent any significant over- or under-collections. The Chief Financial Officer (CFO) has the discretion to determine the appropriate action to

recover any loss to the WCF, including repayment from STRS appropriated funds in the following fiscal year.

WCF Invested Equipment

- 1) When procuring equipment, especially when it benefits both internal users and external customers, OUs should use Invested Equipment (IE) funding if the equipment will have a useful life of more than one year. The use of IE funds provides an opportunity to spread the cost to all benefiting customers through local overhead rates as well as over a longer time period. The purchasing division or OU repays the WCF through monthly IE loan repayments.
- 2) Permission to purchase or manufacture equipment with Working Capital funds is granted each year to OUs by the CFO in the form of a WCF Invested Equipment allocation. Allocation levels are based on:
 - i. Specific allocations related to initiatives approved in the formal budget process (Special Initiative IE).
 - ii. Amounts available in established OU Discretionary IE lines of credit.
 - iii. Specific requests for use of the NIST shared IE line of credit.
 - iv. The ability of the OU to reimburse the WCF through the monthly IE loan repayments and surcharges (see NIST Administrative Manual Subchapter 8.08).
- 3) OU Directors are responsible for reviewing and approving the investment level of each division within their organization. Authorizations must be made/established at the project level.
- 4) At the time that equipment is received or manufactured, the equipment is recorded in the Property System and in the General Ledger Accounts. A useful life is assigned for each capitalized piece of equipment based on guidelines established by the Department of Commerce and NIST.
- 5) Monthly IE loan repayments and the IE surcharge for Discretionary IE purchases are based on the annual loan repayment amounts that OUs provide to the Finance Division. Monthly loan repayments plus surcharges for IE purchases using NIST's shared line of credit are based on a five year repayment schedule provided by the Finance Division.
- 6) Further information on categories and management of equipment is contained [in O 2102.00 Personal Property Management Program](#). Information on IE loan repayments to the WCF is contained in [NIST Administrative Manual Subchapter 8.11, Equipment Financing](#).

Production of Standard Reference Materials

See Directives [NIST O 5601.00 Standard Reference Materials Program](#) and [NIST P 5600.00 Standard Reference Materials Policy](#)

Storeroom Inventories

- 1) NIST maintains inventories of frequently used supplies, materials, equipment, and gases. These inventories are purchased by the WCF and are carried as assets of the Fund. At the time of sale, the cost of the inventory item and a [storeroom replacement surcharge](#) are charged to the buyer's project-task.
- 2) Ceilings are requested by the storeroom management and subsequently approved by the Budget Division for the level of inventory that is to be authorized for the various storerooms (general and metals). The Budget Division also monitors these ceilings to ensure that they are not exceeded. During the year justifications are initiated by storeroom management to the Budget Division should it be determined that an adjustment to the ceilings may be warranted.
- 3) Management of inventories is assigned to the Facilities Services Division.
- 4) Storeroom inventory projects are established in the BUDSTR project type (series 920-939) (see NIST Administrative Manual Subchapter 8.02 Fund Structure Appendices A and B).

DIRECTIVE OWNER

161 – Budget Division

162 – Finance Division

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Edited By	Description of Change
Initial Draft	12/23/2015	Kay Lee	Initial Draft
Ver.01	1/26/2016	Dan Cipra	Incorporated DRB Comments

Scientific Integrity Policy

NIST P 5100.00
Effective Date: 12/16/2011

PURPOSE

Establish the National Institute of Standards and Technology (NIST) Policy on Scientific Integrity.

SCOPE

All NIST Federal employees and Associates engaged in scientific activities at or for NIST.

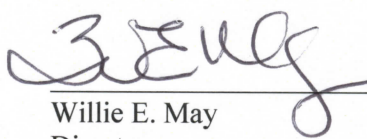
LEGAL AUTHORITY

- [Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635](#)
- [Presidential Memorandum to Heads of Executive Departments and Agencies, dated 03/09/2009](#)
- [Office of Science and Technology Policy Memorandum on Scientific Integrity, dated 12/17/2010](#)
- [2002 Office of Management and Budget \(OMB\) Information Quality Guidelines](#)
- [2005 OMB Information Quality Bulletin for Peer Review](#)

POLICY

It is NIST Policy to promote scientific integrity by creating a culture of personal and organizational responsibility where the practice and management of scientific research and of its products are free from undue influences that are not essential to the practice of science such as personal or social allegiances, beliefs or interests.

The Associate Director for Laboratory Programs is responsible for ensuring that requirements, processes and procedures are developed, implemented and maintained that encourage personal and organizational responsibility in upholding scientific integrity at NIST


Willie E. May
Director

7/24/15
Date

Scientific Integrity

NIST O 5101.00
Effective Date: 01/17/2013

PURPOSE

This directive describes the requirements and responsibilities for the NIST Scientific Integrity Policy. It describes NIST-wide principles to guide and ensure the integrity of the scientific process at the Institute, to ensure the integrity of scientific information, and to engender public trust in NIST's efforts to advance measurement science, standards, and technology.

APPLICABILITY

All NIST Federal Employees and Associates engaged in scientific activities at or for NIST.

REFERENCES

- [Executive Order 13526 - Classified National Security Information](#)
- [Presidential Memo on Scientific Integrity](#)
- Department of Commerce
 - DoC Memo on Scientific Integrity– March 30, 2012
 - [DAO 219-1, Public Communications](#)
 - [DAO 218-1, Legislative Activities](#)
 - [DAO 218-2, Legislative and Intergovernmental Affairs](#)
 - [DAO 218-3, Reports to Congress Required by Law](#)
 - [DAO 219-4, Publications and Audiovisuals Control System](#)
- [Information Quality Act \(Pub. L. 106-554\)](#)
- [NIST P 5100.00 Scientific Integrity](#)
- [NIST O 1801.00 Review of Fundamental Research Communications](#)
- [NIST Administrative Manual Subchapter 3.02 Procedures for Approval of NIST Memberships and Staff Participation in Professional Organizations](#)
- [National Institute Of Standards and Technology Guidelines, Information Quality Standards, and Administrative Mechanism](#)

DEFINITIONS

Scientific integrity - an attribute of institutional and personal behavior in the practice or management of scientific research and of its products, that is free from personal, political or social allegiances, beliefs or interests that are inessential for the practice of science.

The following are taken into account in considering scientific integrity:

- Types of interference include, but are not limited to, political convictions, religious beliefs and economic motivations.
- Belief in a scientific theory, based on scientific practice and consistent with empirical evidence, may legitimately constrain scientific practice, provided it does not prevent empirically testing the validity of the very theory that is the object of such belief.
- NIST's economic motivations may legitimately be used to establish priorities for scientific research, provided they are consistent with NIST's mission and are not otherwise used to suppress scientific findings that may have economic impact deemed adverse to individual, corporate or other interests.
- The practice and management of scientific research and of its products may legitimately be constrained by contractual obligations freely entered upon prior to the conduct of such research, by the institutions and individuals practicing or managing such research.
- Constraints mentioned above include, but are not limited to, those that are part of the terms of employment in the civil service in general, and at NIST in particular, and the technical programs in science, technology, and standards that the U.S. Congress, the U.S. Department of Commerce and NIST management determine should be pursued in the execution of NIST's mission.
- The distortion, alteration, concealment, censorship, or suppression of valid products of *bona fide* scientific research, or the placement of restrictions on the dissemination of such products, by NIST management or by individual NIST scientists, violates scientific integrity, except for those restrictions on dissemination contemplated in the preceding bullets.
- Scientific research is the process of developing scientific knowledge. "Science" and "scientific knowledge" are objects of the philosophy of science. For relevant definitions and discussion, refer to: Philosophy of Science, in, R. Audi (ed.), The Cambridge Dictionary of Philosophy, 2nd Ed., pages 700–704, Cambridge University Press, Cambridge, UK, 1999; C. Hempel, Philosophy of Natural Science, Prentice Hall, Upper Saddle River, NJ, 1966.

PRINCIPLES AND REQUIREMENTS

Integrity is a core value at NIST, and is essential for performing the NIST mission at the highest level. As a result, NIST management and staff must be committed to performing NIST scientific activities with the following considerations:

Scientific Research Excellence:

- NIST scientific work is to be carried out by its scientists, engineers and technical experts with a commitment to intellectual honesty, objectivity, clarity, openness, reproducibility and personal responsibility for one's actions.
- The discussion, presentation and publication of research results shall be subject to the level of peer review required to ensure the quality of such results.
- Management must provide leadership to create an environment that supports the highest levels of research excellence.
- NIST will ensure that those who raise or report concerns about the integrity of NIST scientific work are not subjected to retribution.

Conflict and Bias:

- Scientific work should not be interfered with or biased by commercial, financial, social, religious, political or cultural concerns that are external to the scientific process.
- Individual and organizational conflicts of interest must be actively managed.

Freedom to Disseminate:

- There should be no non-scientific interference in reporting the products of scientific work, except where such publication or distribution is prohibited by law or to protect privacy, proprietary information, or national security as defined in Executive Order 13526.
- NIST actively supports the wide dissemination of scientific work such as publications in open scientific literature, technical staff participation in various scientific venues and events, and unfettered communication between NIST technical staff and the media or general public to communicate scientific results consistent with Department of Commerce policies.
- Measurement results and other data supporting published research results and the development of technology and standards will be made publicly available and will be sufficiently documented to facilitate the reproducibility of the research.

Professional Development:

- NIST contributes to scientific integrity broadly by encouraging its scientists and engineers to provide technical advice through activities such as peer review of journal articles and participation on editorial boards, technical review panels and scientific advisory bodies.
- NIST supports full participation in professional or scholarly societies, committees, task forces and other specialized bodies of professional societies, including serving as officers or on governing boards of such societies with proper legal review and approval as per NIST Administrative Manual Subchapter 3.02.

- NIST recognizes the importance of scientific leadership, growth and recognition as critical components to create a culture that promotes scientific integrity and advances the NIST mission.

RESPONSIBILITIES

NIST Director

- Sets NIST scientific integrity policy.

NIST Associate Director for Laboratory Programs

- Authorized by the Director to determine how the NIST scientific integrity policy is implemented to meet expectations and create the desired environment.
- Ensures the implementation of notices, orders, procedures and guidance related to scientific integrity in the Directive Management System.
- Monitors the institutional environment to maintain and improve the culture of scientific integrity.
- Administers processes and procedures that promote and protect scientific integrity.

OU Directors

- Ensure implementation of, compliance with and accountability for the aspects of the NIST scientific integrity policy for which they are responsible in accordance with procedures issued under this order.
- Provide leadership in support of responsible scientific conduct.

NIST Federal Employees and Associates

- Protect the integrity of the scientific research performed at NIST by adhering to the procedures and principles related to scientific integrity in the Directives Management System.

DIRECTIVE OWNER

600 - Associate Director for Laboratory Programs

APPENDICES

Appendix A: Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/14/2012	Richard Cavanagh (SPO)	First Draft
Ver .01	12/7/2012	Dan Cipra	Incorporated changes and moved Appendix A to the references section
Ver .02	12/18/2012	Dan Cipra	Incorporated OCC comments.
Ver. .03	1/4/2013	Richard Cavanagh	Incorporated DRB comments

Reporting and Resolving Allegations Regarding Violations of Scientific Integrity

NIST PR 5101.01
Effective Date: 6/6/2014

PURPOSE

This directive establishes procedures for reporting and resolving allegations regarding violations of scientific integrity at the National Institute of Standards and Technology (NIST).

APPLICABILITY

This directive is applicable to all NIST Federal employees and Associates engaged in scientific activities at or for NIST, to the extent allowed by law and the terms of the Associate's agreement.

REFERENCE

[NIST O 5101.00 NIST Scientific Integrity](#)

[Department of Commerce Scientific Integrity Memorandum](#)

DEFINITIONS

Complainant(s) - A person(s) or organization(s) who makes an allegation that scientific integrity has been violated.

Good faith allegation – An allegation made with the honest belief that a violation of scientific integrity may have occurred. An allegation is not in good faith if it is made with reckless disregard for or willful ignorance of facts that would disprove the allegation.

NIST Scientific Integrity Officer (NSIO) - A senior career NIST Federal employee with scientific and/or scholarly credentials who reports to the Associate Director for Laboratory Programs.

NIST Integrity Inquiry Team - A team of one or more NIST Federal employees assembled by the NSIO to examine allegations regarding violations of scientific integrity that fall under NIST O 5101.00 and have been determined to warrant investigation.

Office of the Inspector General (OIG) – The Department of Commerce (DoC) Office of the Inspector General (OIG). The office in the Department of Commerce responsible for oversight of programs and operations

Respondent(s) - The person(s) against whom an allegation of violation of scientific integrity is directed or the person whose actions are the subject of the inquiry or investigation.

Scientific integrity – See [NIST O 5101.00](#). .

RESPONSIBILITIES

Chief Counsel for NIST

- Serves as the initial input official for all allegations that a violation of scientific integrity has occurred that is related to NIST.
- Determines whether an allegation can be addressed within NIST, or whether the nature of the allegation requires that it be addressed outside NIST, for example, at the Department of Commerce level.

NIST Scientific Integrity Officer

- Implements the DoC Scientific Integrity Policy as it pertains to NIST.
- Implements the NIST Scientific Integrity Policy.
- Keeps the NIST Director and Chief Counsel informed on the status of the implementation of this directive.
- Coordinates inquiries, investigations, and actions with the Employee Relations (ER) specialist in the Office of Human Resources Management (OHRM).
- Chairs and appoints members of NIST Integrity Inquiry Teams.
- Sequesters evidence related to allegations.
- Represents NIST on interagency issues of scientific integrity
- Provides training for members of inquiry teams.

Complainant

- Makes allegations in good faith, and cooperates with and maintains the confidentiality of the inquiry and investigation processes.

Respondent

- Maintains confidentiality and cooperates with the conduct of the inquiry and investigation.

PROCEDURES

- A. Reporting an Allegation. Allegations of violations of scientific integrity with respect to all NIST Federal employees and Associates engaged in scientific activities at or for NIST shall be submitted in writing. Allegations may be submitted by complainant(s) internal or external to NIST. Examples of violations include, but are not limited to, constraints on Public Communication of research results, unwarranted restrictions on Professional Development, and inappropriate Federal Advisory Committee operations.

Any allegation of violation of scientific integrity shall be submitted to the Chief Counsel for NIST and contain the following information:

- 1) The name, affiliation, and signature of the complainant(s) submitting the allegation and the name and organization of the respondent(s) alleged to have committed the violation.
- 2) A description of the allegation that includes the date, circumstances, and location of the alleged violation.
- 3) Any documents or other relevant items (such as reports, memos, etc.) with annotation showing specifically how the item relates to the allegation.
- 4) An explanation of how the allegation relates to violation of scientific integrity.

Allegations may be returned if they do not contain the above information.

Upon receipt of the properly filed allegation, the Chief Counsel will establish a file to track progress of the allegation until its resolution.

- B. Initial Review. The Chief Counsel will perform an initial review of the allegation within 10 business days of receiving a complete submission. Allegations against NIST management, NIST Federal employees and NIST Associates engaged in scientific activities at or for NIST will be referred to the NSIO for further review, inquiry and investigation, if warranted in the judgment of the Chief Counsel. Allegations against the NIST Director or NIST Associate Directors, if referred, will be referred to the Department of Commerce and shall not be investigated internally by NIST. The Chief Counsel will provide written notice to the complainant(s) notifying them of the status of their allegation and to whom it has been referred within 5 business days of completion of the initial review.
- C. NSIO Review. The NSIO will conduct a review of the allegations and submitted materials within 10 business days of receiving a complete submission to determine if the allegation is covered under the provisions of NIST O 5101.00 and whether an inquiry is warranted. Allegations that have been previously resolved will not be reopened unless substantial new information is submitted. If the NSIO determines that the allegation does not warrant investigation, the NSIO will dismiss the allegation. Written notice of this determination will be provided to the complainant(s) with a copy to the Chief Counsel.
- D. NIST Inquiry. The NSIO will lead an inquiry to determine if there is merit to the allegation.
- 1) The NSIO will inform the NIST Director and NIST Chief Counsel when an inquiry into an alleged violation of scientific integrity has been initiated.
 - 2) The NSIO will identify and inform the manager(s) responsible for the respondent(s) and their management chain up thru their Associate Director, indicating that an

inquiry into an allegation of violation of scientific integrity has been initiated against the respondent. (s) The responsible manager will usually be the supervisor, except when the supervisor feels that a real or perceived conflict of interest exists, in which case another appropriate responsible manager will be identified by the NSIO.

- 3) The NSIO, working with the responsible manager, will form an inquiry team and will conduct an inquiry to determine if the allegation is covered under the provisions of NIST O 5101.00. The NSIO will provide consistency, oversight, and guidance throughout the entire process.
- 4) The NSIO will then notify the respondent(s) in writing (Appendix A - Sample Notification of Allegation of Violation of Scientific Integrity) that an allegation of violation of scientific integrity has been received. The notification shall be conducted privately and preferably in person. At the time of notification, the NSIO and manager will ensure that all original records and materials relevant to the allegation are immediately sequestered.
- 5) If the NSIO determines that the investigation cannot be completed in 120 days, the NSIO will submit to the OCC a written request for an extension that explains the delay, reports on the progress to date, estimates the date of completion of the report, and describes other necessary steps to be taken. If the request is granted, the Research Integrity Officer will file periodic progress reports as requested by the OCC.
- 6) Throughout the inquiry and fact finding, confidentiality must be maintained and identities of the respondent(s) and complainant(s) will be protected.

E. Potential outcomes of inquiry into an allegation of violation of scientific integrity.

- 1) If the NSIO establishes through the inquiry that there is no merit to the charge of a violation of scientific integrity, the case will be dismissed and closed. The NSIO will issue a memorandum through the supervisor to the respondent(s) which notifies the respondent(s) of the dismissal and closure. (Sample Closure Memorandum - Appendix B). A separate memorandum will be issued to the complainant(s) which notifies the complainant that the case is closed. (Sample Closure Memorandum - Appendix C).
- 2) If the NSIO finds incontrovertible evidence that a violation occurred, and that there is no need for further fact finding, the NSIO will issue a memorandum to the NIST Director giving notice of the Violation of Scientific Integrity (Sample Violation of Scientific Integrity Memorandum – Appendix D).
- 3) If the NSIO determines that there appears to be merit to the allegation, and that a formal review and further fact finding by the OIG is required to determine the validity of the allegation and the extent and nature of the alleged violation, then the NSIO will

notify the manager, the respondent(s), the complainant(s), the NIST Chief Counsel, and the OIG.

- 4) All notifications and memoranda that are outcomes of the inquiry shall be issued by the NSIO within 10 business days of closure of the inquiry.

F. Corrective Actions.

- 1) If the incident that led to the allegation of a violation is determined to have resulted in an impact to the integrity of the science, the NSIO and the manager will take steps to correct the loss of integrity and to prevent future occurrences of the sequence of events that led to the impact to integrity. These steps shall include a notice on the NIST internal web site home page, and may include such additional steps or forms of notification as the NSIO deems appropriate after reviewing the impact of the incident and any input from the complainant.
- 2) If the allegation is dismissed, the NSIO will take steps to restore any harm caused by the allegation.

G. Disciplinary Actions (NIST Federal Employees and Associates).

- 1) For NIST Federal employees, the responsible manager and ER Specialist will work together to determine the appropriate action to be taken using the Departmental Directive DAO 202-751 - Discipline, and any union contracts, as applicable.
- 2) For NIST Associates, the sponsor and their line management up to and including the appropriate Associate Director will determine the appropriate action, which may include loss of privileges or termination of their Associate agreement, and/or referral to the Associate's home institution.

H. Appeal Rights (NIST Federal Employees). If disciplinary action is taken against an employee, he or she may have appeal rights under Departmental Directive DAO 202-751- Discipline, and any union contracts, as applicable. Employees should contact their ER Specialist for additional information.

I. Process Flow. A schematic diagram of the NIST response to an allegation that there has been a violation of scientific integrity is provided in Appendix E.

DIRECTIVE OWNER

600 - Associate Director for Laboratory Programs

APPENDICES

- A. Sample Notifications of Allegation of Violation of Scientific Integrity
- B. Sample Closure Memorandum to Respondent
- C. Sample Closure Memorandum to Complainant
- D. Sample Violation of Scientific Integrity Memorandum to the NIST Director

- E. Process Flow Diagram
- F. Revision History

APPENDIX A

SAMPLE NOTIFICATION OF ALLEGATION OF VIOLATION OF SCIENTIFIC INTEGRITY

TO: Respondent

FROM: NIST Scientific Integrity Officer

CC: Chief Counsel, AD, OU Director and Manager

SUBJECT: Allegation of Violation of Scientific Integrity

It is NIST Policy to promote scientific integrity by creating a culture of personal and organizational responsibility where the practice and management of scientific research and its products are free from undue influences that are not essential to the practice of science such as personal or social allegiances, beliefs or interests.

An allegation of violation of scientific integrity has been filed with NIST regarding the following: *Insert as specific and detailed a description of the allegation as possible here, but do not disclose the name or other personally identifiable information of the person(s) who filed the allegation.*

This allegation has not yet been investigated or determined to have merit. However, pursuant to NIST's scientific integrity policy, I will be conducting an inquiry to determine its merits. You must preserve and provide to my office all original research records and materials relevant to the above allegation.

An interview will be scheduled with you to discuss the allegation and will be part of the official record. You may also provide for the record a written response to the allegation. If you chose to provide a written response, it must be submitted to the NSIO within two weeks following your interview date, unless an extension is granted by the NSIO based on your written request submitted in advance of that deadline.

Once an inquiry into this matter is concluded, I will inform you in writing that: (1) a review of this matter has dismissed the allegation and the matter is closed; (2) in the course of the inquiry of this matter, it has been verified that a violation of scientific integrity has taken place and you will be contacted about possible additional action; or (3) the allegation has been referred to the DoC's Office of the Inspector General for further fact-finding.

I have attached a copy of the NIST Directives P 5100.00, O 5101.00 and PR 5101.01, on Scientific Integrity. Please review them carefully and let me know if you have any questions about this process.

APPENDIX B

SAMPLE CLOSURE MEMORANDUM TO RESPONDENT

TO: Respondent

Through: Supervisor

FROM: NIST Scientific Integrity Officer

SUBJECT: Resolution of Allegation of Violation of Scientific Integrity

After an inquiry into the allegation of violation of scientific integrity that was filed against you, I have found the allegation to be without merit. *(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).* As a result, the inquiry into the concerns reflected in this allegation is considered closed. I appreciate your cooperation in this important process.

APPENDIX C

SAMPLE CLOSURE MEMORANDUM TO COMPLAINANT

TO: Complainant

FROM: NIST Scientific Integrity Officer

SUBJECT: Resolution of Allegation of Violation of Scientific Integrity

After an inquiry into the allegation of violation of scientific integrity that you filed against, I have found the allegation to be without merit. ***(Insert as specific and detailed a description of the allegation)***. As a result, the inquiry into the concerns reflected in this allegation is considered closed. I appreciate your cooperation in this important process.

APPENDIX D

SAMPLE VIOLATION OF SCIENTIFIC INTEGRITY MEMORANDUM TO THE NIST DIRECTOR

TO: NIST Director

FROM: NIST Scientific Integrity Officer

CC: Chief Counsel, AD, OU Director

SUBJECT: Violation of Scientific Integrity

I am informing you that, in the course of an inquiry into the allegation of violation of scientific integrity that was filed against, I have found incontrovertible evidence supporting the charge. *(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).*

The respondent *(explain nature of incontrovertible evidence – admission by respondent, etc.)*

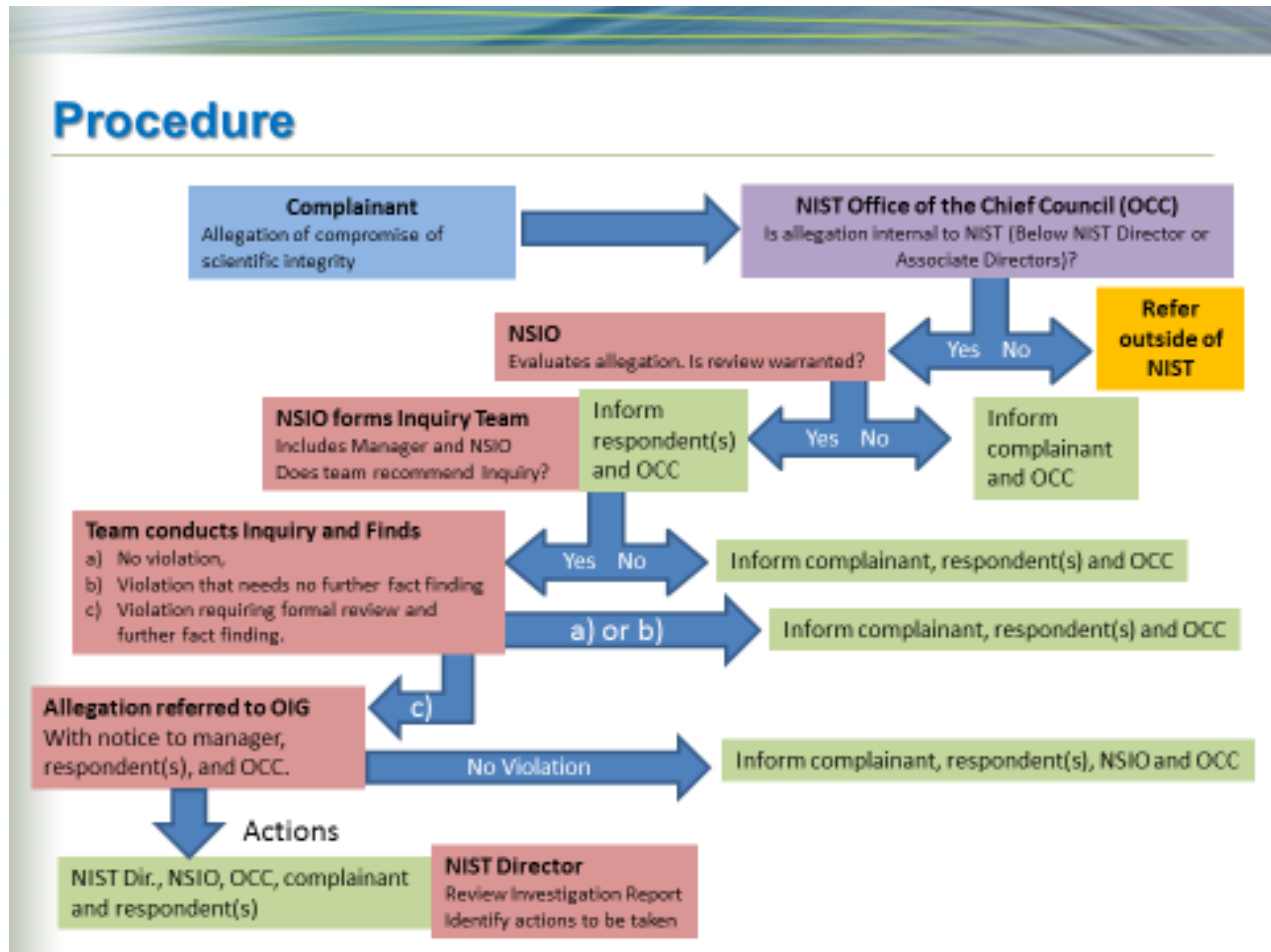
As a result, it is recommended that NIST management pursue administrative actions commensurate with the severity *(insert a brief summary of the implications of this violation, being clear to address intent)*

It is also recommended that NIST management take immediate steps to correct the loss of integrity and prevent future occurrences of the sequence of events that led to the impact to integrity. *(Include specific steps to publicly correct the violation to the identify the respondent that will prevent future occurrences)*

APPENDIX E:

PROCESS FLOW DIAGRAM

The diagram below represents the process flow for NIST response to alleged violations of Scientific Integrity



APPENDIX F:

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	3/25/2014	Richard Cavanagh (SPO)	First Draft following input from: Jim St. Pierre, Lloyd Whitman, Henry Wixon, Sheila Nichols, Paul Zielinski
Ver .01	4/8/2014	Dan Cipra	Incorporated all changes.
Ver .02	4/11/2014	Dan Cipra	Accepted all OSP and OCC comments
Ver .03	5/19/14	R. Cavanagh	Changes based on DRB Comments.
Ver .04	5/20/14	R. Cavanagh	Changes based on DRB Meeting feedback and discussion. The changes also affected O 110.

Responsible Conduct of Research

NIST P 5200.00
Effective Date: 11/26/2014

PURPOSE

To establish the National Institute of Standards and Technology (NIST) policy on striving for and promoting excellence and rigor in the conduct of its research activities.

SCOPE

All NIST employees and Associates engaged in research activities at or for NIST, to the extent allowed by law and the terms of the Associate's agreement.

LEGAL AUTHORITIES AND REFERENCES

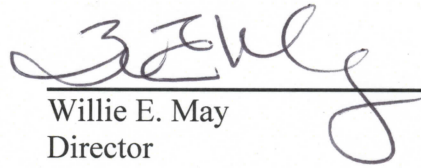
- [Executive Office of the President; Federal Policy on Research Misconduct; Preamble for Research Misconduct Policy](#); 65 FR 76260-76264 (Dec. 6, 2000)
- [Treasury and General Government Appropriation Act for Fiscal Year 2001](#), Pub. L. No. 106-554, § 515 Appendix C, 114 Stat. 2763A-153 (2000)
- [Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility and Integrity of Information Disseminated by Federal Agencies](#), Office of Management and Budget (OMB) 67 FR 8452 (Feb. 22, 2002)
- [OMB Final Information Quality Bulletin for Peer Review](#) (Dec. 16, 2004),
- [Standards of Ethical Conduct for Employees of the Executive Branch](#), 5 C.F.R. Part 2635
- [NIST Information Quality Standards and Guidelines](#)

POLICY

It is NIST Policy to strive for and promote excellence and rigor in its research activities by:

- Ensuring that all research conducted or supported by NIST is carried out in ways that are reproducible and that guarantee the quality and reliability of research products;
- Ensuring that the research is conducted responsibly and ethically;
- Ensuring that research products are appropriately subject to peer evaluation and open to public scrutiny; and
- Creating an environment where research is conducted ethically and where suspected incidents of non-compliant conduct are addressed.

The Associate Director for Laboratory Programs is responsible for ensuring that requirements, processes and procedures are developed, implemented and maintained that encourage personal and organizational responsibility in upholding responsible conduct of research at NIST.


Willie E. May
Director

7/24/15
Date

Responsible Conduct of Research Order

NIST O 5201.00
Effective Date: 11/25/2014

PURPOSE

This directive describes the requirements and responsibilities under the NIST Policy for Responsible Conduct of Research. It describes NIST-wide principles to guide and ensure that the scientific research conducted at NIST or supported by NIST is undertaken with the highest regard for an unadulterated research record and protection of the interests of those involved in that research.

APPLICABILITY

This directive is applicable to all NIST employees and Associates engaged in research activities at or for NIST, to the extent allowed by law and the terms of the Associate's agreement.

REFERENCES

- [Department of Commerce "Standard Terms and Conditions for Financial Assistance"](#) January 2013
- [NIST Responsible Conduct of Research Policy](#), NIST P 5200.00
- [Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, Other Non-Profit and Commercial Organizations, as codified by the Department of Commerce, 15 CFR Part 14](#)
- [Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments, as codified by the Department of Commerce, 15 CFR Part 24](#)
- [The Common Rule for the Protection of Human Subjects, as codified by the Department of Commerce, 15 CFR Part 27](#)
- [The Animal Welfare Act, 7 U.S.C. 54, §2131-2156, as amended](#)
- The [International Ethical Guidelines for Biomedical Research Involving Human Subjects](#) (Council for International Organizations of Medical Sciences, 2002)
- [Health Research Extension Act of 1985](#)
- [Office of Science and Technology Policy \(2000\): Federal Policy on Research Misconduct: Notification of Final Policy. Federal Register December 6, 2000 65\(235\): 76260-76264.](#)
- [NIST Investigating Suspected Misuse of IT Resources](#), O 6104.00
- [NIST Access and Use of IT Resources](#), O 6103.00

DEFINITIONS

Adjudication - The reviewing of recommendations and determination of appropriate corrective actions.

Allegation - Any written statement, having a self-identified author, describing possible research misconduct and given to the NIST Responsible Conduct Officer (RCO).

Claimant(s) - A person who makes an allegation of research misconduct.

Deciding Official (DO) - The NIST official who makes the final determination on allegations of research misconduct and any responsive institutional actions.

Fabrication - Making up data or results and recording or reporting them.

Falsification - Manipulating research materials, equipment, or processes or changing or omitting data or results such that the research is not accurately represented in the research record.

Good faith allegation - An allegation made with the honest belief that research misconduct may have occurred. An allegation is not in good faith if it is made with reckless disregard for or willful ignorance of facts that would disprove the allegation.

Human Subject - A living individual about whom a research investigator (whether professional or student) conducting research obtains: 1) data through intervention or interaction with the individual, or 2) identifiable private information.

Humane care and treatment of Animals in Research - Encompasses the caring for and use of animals in ways judged to be scientifically, technically, and humanely appropriate.

Inquiry - The assessment of whether an allegation of research misconduct has substance and if an investigation is warranted. The purpose of the inquiry is not to reach a final conclusion with respect to a finding of research misconduct.

Inquiry Committee - A committee consisting of individuals who do not have unresolved personal, professional, or financial conflicts of interest with those involved with the inquiry and should include individuals with the appropriate scientific expertise to evaluate the evidence and issues related to the allegation, interview the principals and key witnesses, and conduct the inquiry.

Inquiry Official - Identified by the Research Conduct Officer (RCO) for each inquiry and is the lowest level line manager to whom either both the respondent and claimant report, or is a line manager to whom neither the respondent nor claimant report.

Investigation - The formal development of a factual record, and the examination of that record leading to dismissal of the case or to a recommendation for a finding of research misconduct or other appropriate remedies. The investigation will also determine whether there are additional instances of possible misconduct that would justify broadening the scope beyond the initial allegations.

Investigation Committee - A committee consisting of individuals who do not have unresolved personal, professional, or financial conflicts of interest with those involved with the investigation and should include individuals with the appropriate scientific expertise to evaluate the evidence and issues related to the allegation, interview the respondent and claimant and conduct the investigation. Individuals appointed to the investigation committee may also have served on the inquiry committee.

Plagiarism - The appropriation of another person's ideas, processes, results, or words without giving appropriate credit.

Research Conduct Officer (RCO) - The institutional official responsible for assessing allegations of research misconduct and determining when such allegations warrant inquiries and for overseeing any inquiries and investigations.

Research Record - Comprises data or results that embody the facts resulting from scientific inquiry and technological development, and includes, but is not limited to, research proposals and grant applications (funded or not), laboratory records and prototypes (both physical and electronic), computer files and printouts, computer programming codes, progress reports, abstracts, theses, oral presentations, internal reports, and journal articles.

Research misconduct - The fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results. It does not include honest error or differences of opinion.

Respondent(s) - The person(s) against whom an allegation of research misconduct is directed or the person whose actions are the subject of the inquiry or investigation.

Retaliation - Any action that adversely affects the employment or other status of an individual that is taken by an institution or an employee because the individual has, in good faith, made an allegation of research misconduct or of inadequate institutional response thereto, or has cooperated in good faith with an investigation of such allegation.

PRINCIPLES AND REQUIREMENTS

Advances in science, engineering, and all fields of research depend on the reliability of the research record, as do the benefits associated with them in areas such as commerce and national security. Sustained public trust in the research enterprise also requires confidence in the research record, in the processes involved in its ongoing development, and in the ethical treatment of those involved in that research. Research conducted or supported by NIST must be conducted in a manner that instills confidence in research findings, underscores the reliability of research findings, and protects the interests of individuals and organizations who participate in the research. This directive establishes the scope of NIST's interest in the accuracy and reliability of the research record, the processes involved in its development, and the ethical treatments of the subjects of that research. It contains a definition of research misconduct and delineates the

responsibilities for ensuring scientific research excellence and responsible conduct of research conducted or supported by NIST.

To create an environment where research is conducted responsibly:

- NIST will examine, resolve, and report all reasonable allegations of research misconduct. The processes will protect the rights and privacy of those accused.
- NIST will protect human and animal subjects who are involved in NIST conducted or NIST supported research.
- All those conducting research at or for NIST will report observed, suspected, or apparent research misconduct to their line management and/or the NIST RCO. If an individual is unsure whether a suspected incident falls within the definition of research misconduct, he or she may meet with or contact the RCO to discuss the suspected research misconduct informally, which may include discussing it anonymously and/or hypothetically.
- All those conducting research at or for NIST will cooperate with their institutional officials in the review of allegations and the conduct of inquiries and investigations.
- NIST shall limit disclosure of the identity of respondents and claimants to those who need to know in order to carry out a thorough, competent, objective, and fair research misconduct proceeding.
- No one subject to this directive may retaliate in any way against claimants, witnesses, or committee members. Any alleged or apparent retaliation against claimants, witnesses or committee members should be reported immediately to the RCO, who shall review and, as necessary, refer the matter, and who shall make all reasonable and practical efforts to counter any potential or actual retaliation and protect and restore the position and reputation of the person against whom the retaliation is directed.
- As requested and as appropriate, NIST shall make all reasonable and practical efforts to protect or restore the reputation of persons alleged to have engaged in research misconduct, but against whom no finding of research misconduct is made.
- Throughout the research misconduct proceeding, NIST will review the situation to determine if there is any threat of harm to public health, federal funds and equipment, or the integrity of the NIST supported research process. In the event of such a threat, NIST will take appropriate interim administrative actions to protect against any such threat.

A finding of research misconduct requires that:

- There be a significant departure from accepted practices of the relevant research community; and
- The misconduct be committed intentionally, or knowingly, or recklessly; and
- The allegation must be proved by a preponderance of evidence.

Protection of intellectual property rights, scientific integrity, and the safety of NIST staff and Associates are treated in separate directives.

Authorship is addressed differently by different professional societies. It should not be assumed that all those who contribute to a scientific document will have the same perception as to the level of contribution that warrants credit as an author. Authorship disputes are not covered by this policy unless they involve plagiarism (see [OSTP 2000](#)). More information on Authorship is found [here](#).

RESPONSIBILITIES

NIST Director

- Sets NIST Policy for responsible conduct of research.

NIST Associate Director for Laboratory Programs

- Authorized by the NIST Director to determine how the NIST Policy for responsible conduct of research is implemented to meet expectations and create the desired environment for Laboratory Programs.
- Ensures the implementation of notices, orders, procedures, and guidance related to responsible conduct of research in the Directives Management System.
- Monitors the institutional environment to address suspected incidents of research misconduct.
- Administers processes and procedures that address allegations of research misconduct.
- Serves as the Deciding Official (DO) for NIST regarding NIST research misconduct matters.
- Appoints the NIST RCO.
- Has written policies and procedures for responding to allegations of research misconduct, as required by NIST O 5201.00.

Deciding Official (DO)

- The DO will receive the investigation report and, after consulting with the RCO and/or other NIST officials, decide the extent to which NIST accepts the findings of the investigation and, if research misconduct is found, decide what, if any, institutional administrative actions are appropriate.

Inquiry Official (IO)

- The IO will receive the inquiry report and after consulting with the RCO and/or other institutional officials, decide whether an investigation is warranted.
- Any finding that an investigation is warranted must be made in writing by the IO. If it is found that an investigation is not warranted, the IO and the RCO will ensure that detailed documentation of the inquiry is retained according to the NIST record retention schedule.

NIST Research Conduct Officer (RCO)

- The RCO has primary responsibility for implementation of the institution's policies and procedures on responsible conduct of research.
- Coordinates with other institutions when allegations arise that involve NIST and non-NIST staff.
- Informs institutional members about its research misconduct policies and procedures and NIST's commitment to compliance with those policies and procedures.
- Takes appropriate interim action during a research misconduct proceeding to protect public health, federal funds and equipment, and the integrity of the NIST supported research processes.
- Takes all reasonable and practical steps to foster a research environment that promotes the responsible conduct of research, research training, and activities related to that research or research training, discourages research misconduct, and deals promptly with allegations or evidence of possible research misconduct.
- Consults confidentially with persons uncertain about whether to submit an allegation of research misconduct.
- Receives allegations of research misconduct.
- Assesses each allegation of research misconduct to determine if an inquiry is warranted as a result of the allegation falling within the definition of research misconduct, being within the jurisdictional criteria of NIST P 5200.00, and being sufficiently credible and specific so that potential evidence of research misconduct may be identified.
- Appoints an IO for each allegation that is found to be sufficiently credible and specific to warrant an inquiry.
- Convenes an Investigation Team when warranted by an IO. Ensures that an Investigation Report is issued for each investigation.
- In cooperation with other institutional officials, takes all reasonable and practical steps to protect or restore the positions and reputations of good faith claimants, witnesses, and committee members and to counter potential or actual retaliation against them by respondents or other institutional members.
- Makes all reasonable and practical efforts, if requested and as appropriate, to protect or restore the reputation of persons alleged to have engaged in research misconduct, but against whom no finding of research misconduct is made.
- Promptly takes all reasonable and practical steps to obtain custody of all research records and evidence needed to conduct the research misconduct proceeding, inventory the records and evidence, and sequester them in a secure manner.
- Takes all reasonable and practical steps to ensure the cooperation of respondents and other NIST staff and Associates with research misconduct proceedings, including, but not limited to, their providing information, research records and evidence.
- Provides confidentiality to those involved in the research misconduct proceeding as

required by applicable law, and NIST policy.

- Determines whether each person involved in handling an allegation of research misconduct has a personal, professional or financial conflict of interest and takes appropriate action, including recusal, to ensure that no person with such a conflict is involved in the research misconduct proceeding.
- Keeps the DO and others who need to know informed of the progress of the review of the allegation of research misconduct.
- Assists the DO in implementing his/her decision to take administrative action against any claimant, witness, or committee member determined by the DO not to have acted in good faith.
- Maintains records in accordance with 44 U.S.C. Chapters 29 (Records Management by the Archivist of the United States and by the Administrator of the General Services) and 33 (Disposal of Records). All NIST files will follow the guidance outlined in the Comprehensive Records Schedule found [here](#)
- Ensures that administrative actions taken by NIST are enforced and takes appropriate action to notify other involved parties, such as sponsors, law enforcement agencies, professional societies, and licensing boards, of those actions.
- Follows procedures for responding to allegations of research misconduct, as required by NIST PR 5201.01.
- Complies with written policies (NIST P 5200.00) and procedures (NIST PR 5201.01) and the requirements of NIST O 5201.00.

Office of Information Systems Management (OISM) Director

- Supports sequestration and analysis of electronic records during an inquiry or investigation.

Office of Acquisition and Agreements Management (OAAM) Director

- Ensures that all NIST contracts, grants, cooperative agreements, and other agreements contain appropriate provisions to ensure that research supported by NIST is conducted according to the principles of the NIST policy.

Technology Partnerships Office (TPO) Director

- Informs domestic guest researchers of their need to comply with the NIST Policy on responsible conduct of research as found in NIST P 5200.00.

Office of International and Academic Affairs (OIAA) Director

- Informs foreign guest researchers of their need to comply with the NIST Policy on responsible conduct of research as found in NIST P 5200.00.

NIST Line Management

- Ensures implementation of, compliance with, and accountability for responsible conduct of research at NIST and by NIST staff.

- Provides leadership in support of responsible conduct of research.
- Takes all reasonable and practical steps to foster a research environment that promotes the responsible conduct of research, research training, and activities related to that research or research training, discourages research misconduct, and deals promptly with allegations or evidence of possible research misconduct.
- Ensures that all NIST contracts, grants, cooperative agreements, and other agreements contain appropriate provisions to ensure that research supported by NIST is conducted according to the principles of the NIST policy.

NIST Employees

- Adhere to the procedures and principles related to responsible conduct of scientific research in the NIST Directives Management System
- Notify NIST management of suspected incidents of research misconduct.
- Cooperate with institutional responses to allegations of research misconduct.
- Direct all internal or external allegations of research misconduct to the NIST RCO.

NIST Associates

- Adhere to the procedures and principles related to responsible conduct of scientific research in the NIST Directives Management System, as specified in written agreements with NIST.
- Cooperate with institutional responses to allegations of research misconduct.

Claimant

- The claimant is responsible for making allegations in good faith, maintaining confidentiality, and cooperating with the inquiry and investigation. As a matter of good practice, the claimant should be interviewed at the inquiry stage and given the transcript or recording of the interview for correction. The claimant must be interviewed during an investigation, and be given the transcript or recording of the interview for correction.

Respondent

- The respondent is responsible for maintaining confidentiality and cooperating with the conduct of an inquiry and investigation.

DIRECTIVE OWNER

Associate Director for Laboratory Programs

APPENDICES

Appendix A: Supplemental References

Appendix B: Revision History

APPENDIX A

SUPPLEMENTAL REFERENCES

Nothing in this order will be interpreted in a manner that is inconsistent with topics covered in Department of Commerce policies and federal laws listed below:

- Department of Commerce
 - DAO 219-1, “Public Communications”
 - DAO 218-1, “Legislative Activities”
 - DAO 218-2, “Congressional Correspondence and Inquiries”
 - DAO 218-3, “Reports to Congress Required by Law”
 - DAO 219-4, “Publications and Audiovisuals Control System”
 - DAO 203-26 “Department of Commerce Grants Administration”
 - [Department of Commerce Financial Assistance Standard Terms and Conditions](#)
(January 2013)
- Information Quality Act (Pub. L. 106-554)

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	11 June 12	Richard Cavanagh(OSP)	First Draft
Draft	2014	Nicholas Barbosa	Vetted by team
		Timothy Burns	
		Richard Cavanagh	
		Michael H. Kelley	
		Michael Moore	
		Sheila Nichols	
		Henry Wixon	
		David Yashar	
		Nikolai Zhitenev	
Rev .01	11/19/2014	Dan Cipra	Incorporated all DRB changes
Rev. .02	2/18/2015	Dan Cipra	Incorporated OCC Interim Review comments based on DO approval

Procedures in Response to Allegations of Research Misconduct

NIST PR 5201.01
Effective Date: 11/25/2014

PURPOSE

This document establishes procedures to be followed at NIST for reporting or responding to allegations of research misconduct.

APPLICABILITY

This directive applies to allegations directed towards any NIST employee or Associate engaged in research activities at or for NIST, to the extent allowed by law and the terms of the Associate's agreement.

REFERENCES

- [NIST P 5200.00](#) NIST Responsible Conduct of Research Policy
- [NIST O 5201.00](#) NIST Responsible Conduct of Research Order
- [44 U.S.C. Chapters 29](#) Records Management
- [44 U.S.C. Chapters 33](#) Records Disposal
- [NIST Comprehensive records schedule](#)
- Department of Commerce Departmental Administrative Order [\(DAO\) 202-751](#)

BACKGROUND

A finding of research misconduct represents a violation of NIST policy that puts the public trust in NIST's research enterprise at risk. In accordance with NIST P 5200.00 and NIST O 5201.00, NIST has implemented the following processes to ensure a complete and thorough assessment of all allegations of research misconduct when the respondent was working with NIST resource support at the time of the alleged infraction.

Other Considerations

A. Completion of Cases

Generally, all NIST conducted inquiries and investigations will be carried through to completion and all significant issues will be pursued diligently. The Research Conduct Officer (RCO) must notify the Deciding Official (DO) in advance if there are plans to close a case at the inquiry, investigation, or appeal stage on the basis that respondent has admitted guilt, or for any other reason, except: (1) closing of a case at the inquiry stage

on the basis that an investigation is not warranted; or (2) a finding of no misconduct at the investigation stage.

B. NIST Administrative Actions

If the DO determines that research misconduct is substantiated by the findings, he or she will decide on the appropriate actions to be taken, after consultation with the RCO. The administrative actions may include:

- Withdrawal or correction of all pending or published abstracts and papers emanating from the research where research misconduct was found;
- Removal of the responsible person from the particular project, letter of reprimand, special monitoring of future work, probation, suspension, salary reduction, or initiation of steps leading to possible rank reduction or termination of employment in accordance with DAO 202-751;
- Restitution of funds to the grantor agency as appropriate; and/or
- Other appropriate action.

C. Termination or Resignation Prior to Completing Inquiry or Investigation

The termination of the respondent's institutional employment, by resignation or otherwise, before or after an allegation of possible research misconduct has been reported, will not preclude or terminate the research misconduct proceeding or otherwise limit any of the institution's responsibilities under NIST O 5201.00.

If the respondent, without admitting to the misconduct, elects to resign his or her position after NIST receives an allegation of research misconduct, the assessment of the allegation will proceed, as well as the inquiry and investigation, as appropriate based on the outcome of the preceding steps. If the respondent refuses to participate in the process after resignation, the RCO and any inquiry or Investigation Committee will use their best efforts to reach a conclusion concerning the allegations, noting in the report the respondent's failure to cooperate and its effect on the evidence.

D. Restoration of the Respondent's Reputation

Following a final finding of no research misconduct, the RCO must, at the request of the respondent, undertake all reasonable and practical efforts to restore the respondent's reputation. Depending on the particular circumstances and the views of the respondent, the RCO should consider notifying those individuals aware of or involved in the investigation of the final outcome, publicizing the final outcome in any forum in which the allegation of research misconduct was previously publicized, and expunging all reference to the research misconduct allegation from the respondent's personnel file. Any NIST actions to restore the respondent's reputation should first be approved by the DO.

E. Protection of the Claimant, Witnesses and Committee Members

During the research misconduct proceeding and upon its completion, regardless of the finding made with respect to research misconduct, the RCO must undertake all reasonable and practical efforts to protect the position and reputation of, or to counter potential or actual retaliation against, any claimant who made allegations of research misconduct in good faith and of any witnesses and committee members who cooperate in good faith with the research misconduct proceeding. The DO will determine, after consulting with the RCO, and with the claimant, witnesses, or committee members, respectively, what steps, if any, are needed to restore their respective positions or reputations or to counter potential or actual retaliation against them. The RCO is responsible for implementing any steps the DO approves.

F. Allegations Not Made in Good Faith

If relevant, the DO or IO will determine whether the claimant's allegations of research misconduct were made in good faith, or whether a witness or committee member acted in good faith. If the DO or IO determines that there was an absence of good faith he/she will determine whether any administrative action should be taken against the person who failed to act in good faith.

G. Allegations not directed at NIST employees

Allegations against NIST Associates, Visitors, Contractors and Grantees will be addressed by the policies of their home institution. To the extent that access to records that reside at NIST is germane to the resolution process of the home institution, the NIST RCO will provide copies of or access to the pertinent records, in compliance with applicable law.

If the respondent was a NIST employee at the time of the alleged incident, but is no longer a NIST employee, NIST will follow the procedures in this directive.

H. Allegations where the respondents include NIST employees and parties not employed by NIST

For an allegation against multiple respondents, some of whom are NIST employees and some of whom are not NIST employees, the NIST RCO will work with all respondents' RCOs (or equivalent) through the resolution of the allegation, or until a determination is made that NIST employees are removed from consideration as respondents.

I. If the respondent does not have an RCO or equivalent (such as a private party or an independent contractor), the NIST RCO will work with the NIST Organizational Unit (OU) that sponsored the respondent.

PROCEDURES

RECEIPT OF ALLEGATION

A. When an allegation of research of misconduct is made, it goes to the RCO for intake.

- The intake process for allegations directed at NIST Employees is diagramed in Appendix A.

- The intake process for allegations directed at researchers funded or supported by NIST is diagrammed in Appendix B.
- B. The NIST response to all allegations of research misconduct is diagrammed in Appendix C.

ASSESSMENT OF ALLEGATION

- C. The RCO follows the process in Appendix D when assessing all allegations of research misconduct.
- D. If the assessment by the RCO finds that the allegation lacks sufficient credibility or specificity to justify an inquiry, the claimant will be notified of such.

INQUIRY INTO ALLEGATION

- E. If the assessment leads to an inquiry, the RCO sends a notification of inquiry and possible investigation (Appendix E) to the respondent, and obtains an information and acknowledgement confirmation from the NIST employee (Appendix F) or associate (Appendix G), as appropriate.
- F. The RCO assigns a case number to the allegation and establishes an Inquiry Committee, identifies the Chairperson of the Committee and secures confidentiality agreements for all members of the Inquiry Committee (Appendix H).
- G. The RCO identifies an Inquiry Official for the Inquiry.
- H. The RCO directs the Inquiry Committee to conduct an Inquiry following the process in Appendix I, and to develop its report following Appendix J.
- I. If the Inquiry Committee finds that there is no basis for the allegation, the RCO sends a closure memorandum to the respondent (Appendix K) and the claimant (Appendix L).
- J. If the inquiry leads to an investigation, the RCO establishes an Investigation Committee and identifies a Chairperson. The Chairperson of the Investigation Committee sends a notification of investigation to the respondent (Appendix M) and the claimant (Appendix N).

INVESTIGATION OF AN ALLEGATION

- K. The Investigation Committee conducts an investigation following the process in Appendix O and develops an investigation report following Appendix P.
- L. If the Investigation Committee reaches a determination as to whether a finding of research misconduct is warranted, notification is provided to the respondent (Appendix Q) and claimant (Appendix R).
- M. If the Investigation Committee reaches a finding of research misconduct, notification is provided to the respondent (Appendix S), claimant (Appendix T), and the Associate Director of Laboratory Programs (ADLP) (Appendix U).

DIRECTIVE OWNER

600 Associate Director of Laboratory Programs

APPENDICES

Appendix A: Diagram for an allegation directed at a NIST employee

Appendix B: Diagram for an allegation directed at a researcher funded or supported by NIST

Appendix C: Process flow schematic for NIST response to an allegation of research misconduct.

Appendix D: Procedure for Conducting the Assessment

Appendix E: Notification of Inquiry and Possible Investigation of Research Misconduct (Respondent)

Appendix F: Employee Information and Acknowledgment Form

Appendix G: Associate Information and Acknowledgment Form

Appendix H: Confidentiality Agreement for Members of an Inquiry or Investigation Committee

Appendix I: Procedure for Conducting the Inquiry

Appendix J: Procedure for Developing the Inquiry Report

Appendix K: Closure Memorandum to Respondent Following Inquiry

Appendix L: Closure Memorandum to Claimant Following Inquiry

Appendix M: Notification to Respondent of Investigation of Alleged Research Misconduct

Appendix N: Notification to Claimant of Investigation of Alleged Research Misconduct

Appendix O: Procedure for Conducting the Investigation

Appendix P: Procedure for Developing the Investigation Report

Appendix Q: Closure Memorandum to Respondent Following Investigation

Appendix R: Closure Memorandum to Claimant Following Investigation

Appendix S: Research Misconduct Finding Memorandum to the Respondent

Appendix T: Research Misconduct Finding Memorandum to the Claimant

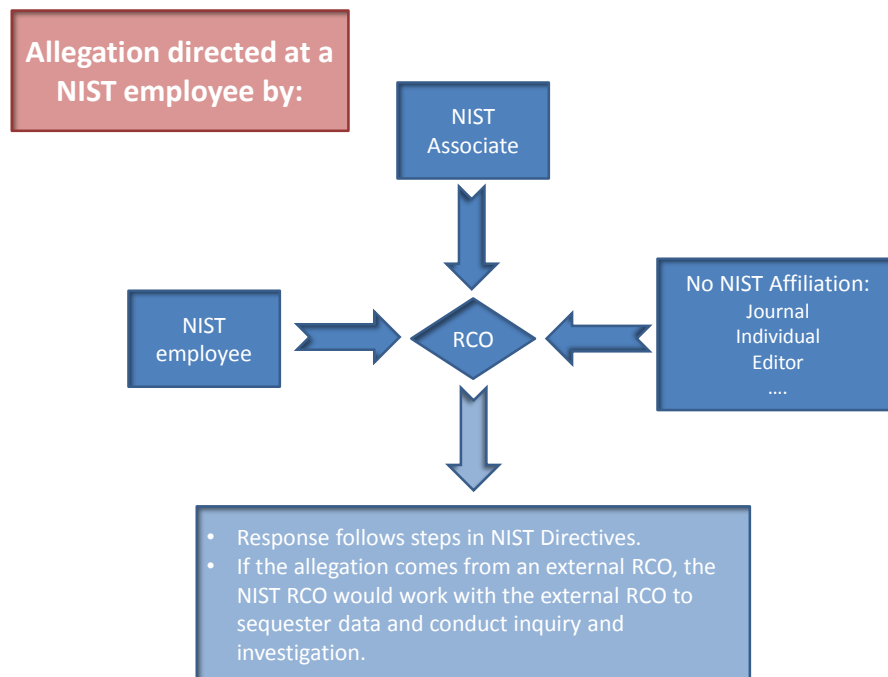
Appendix U: Research Misconduct Memorandum to the ADLP

Appendix V: Revision History

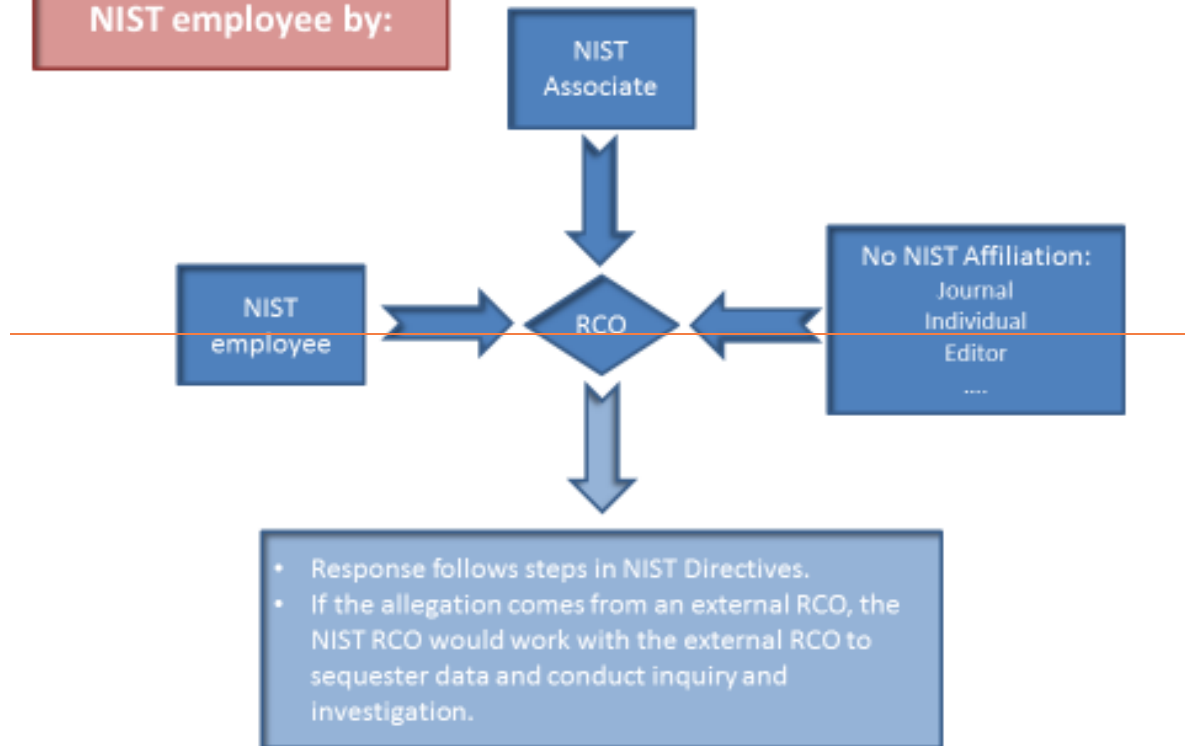
APPENDIX A

DIAGRAM FOR AN ALLEGATION DIRECTED AT A NIST EMPLOYEE

Allegation intake diagram for NIST Research Conduct Officer in response to an allegation directed at a NIST employee.



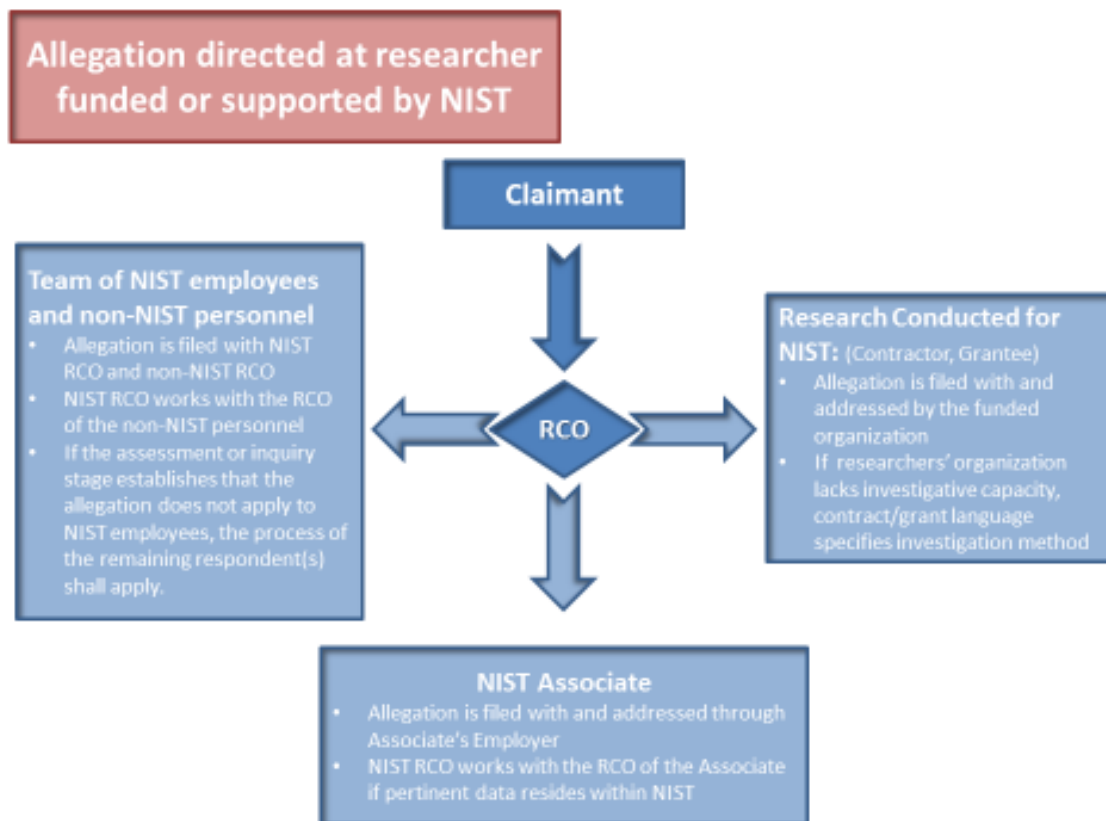
Allegation directed at a
NIST employee by:



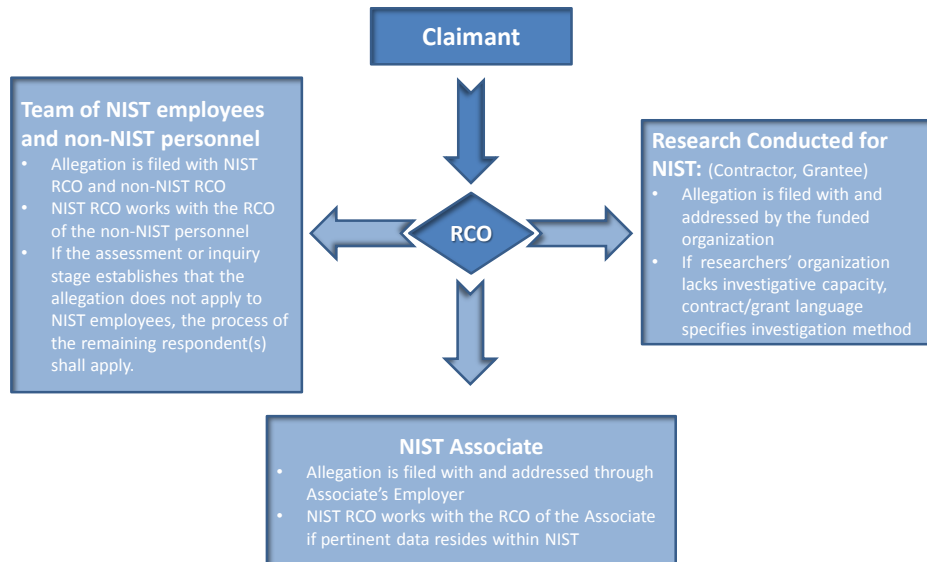
APPENDIX B

DIAGRAM FOR AN ALLEGATION DIRECTED AT A RESEARCHER FUNDED OR SUPPORTED BY NIST

Allegation intake diagram for NIST Research Conduct Officer for an allegation directed at a researcher funded or supported by NIST.

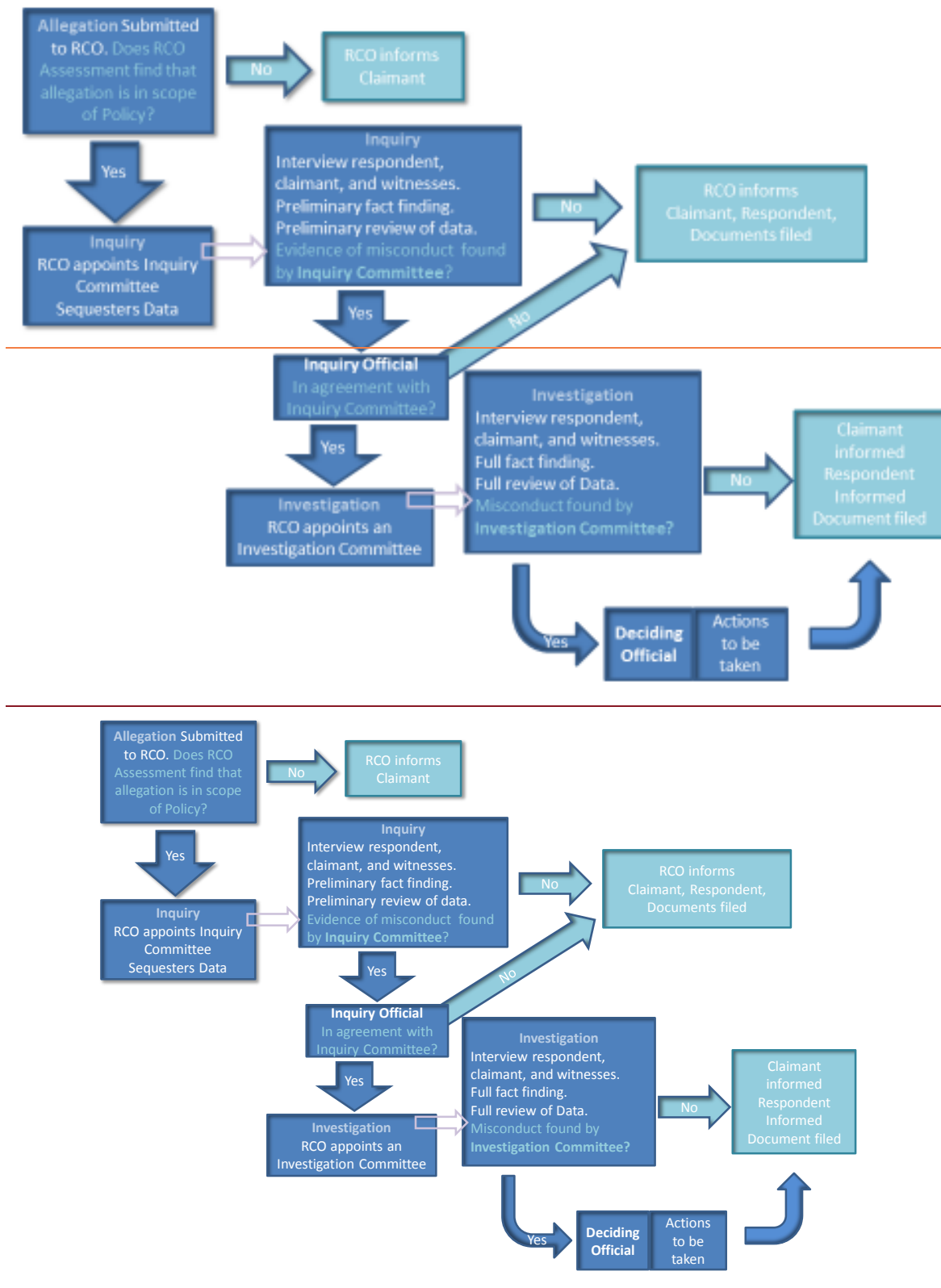


**Allegation directed at researcher
funded or supported by NIST**



APPENDIX C

PROCESS FLOW SCHEMATIC FOR NIST RESPONSE TO AN ALLEGATION OF RESEARCH MISCONDUCT.



APPENDIX D

PROCEDURE FOR CONDUCTING THE ASSESSMENT

A. Assessment of Allegations

Upon receiving an allegation of research misconduct, the RCO will immediately assess the allegation to determine whether any of the respondents were NIST employees at the time of the alleged misconduct. If none of the respondents were NIST employees at the time of the allegation, the RCO will notify the claimant that the allegation will not be addressed by NIST.

If the respondent(s) were not NIST employees at the time of the allegation, the RCO will direct or advise the claimant to contact the respondent's home organization to submit the allegation to the appropriate organizational official.

Any allegation that includes a respondent that was a NIST employee at the time of the alleged research misconduct that is sufficiently credible and specific so that potential evidence of research misconduct may be identified, will be the subject of an inquiry.

In the case of NIST respondents, the RCO shall determine the Group, Division, Organizational Unit (OU) or cross-OU involvement, and communicate with the relevant managers regarding the existence of the allegation.

On or before the date on which the respondent is notified of the allegation, the RCO may obtain custody of, inventory, and sequester all research records and evidence needed to conduct the research misconduct proceeding, as provided in Appendix I.

The assessment period should be brief, preferably concluded within five business days of receipt of the allegation.

In conducting the assessment, the RCO need not interview the claimant, respondent, or other witnesses, or gather data beyond any that may have been submitted with the allegation, except as necessary to determine whether the allegation is sufficiently credible and specific so that potential evidence of research misconduct may be identified.

APPENDIX E

NOTIFICATION OF INQUIRY AND POSSIBLE INVESTIGATION OF RESEARCH MISCONDUCT

TO: Respondent

FROM: NIST Research Conduct Officer

CC: NIST Chief Counsel and Respondent's AD, OU Director and Supervisor

SUBJECT: Allegation of Research Misconduct

It is NIST Policy to strive for and promote excellence and rigor in its research activities by:

- ensuring that all scientific research conducted or supported by NIST is carried out in ways that are reproducible and that guarantee the quality and reliability of research products
- ensuring that the research is conducted responsibly and ethically
- ensuring that research products are subject to peer evaluation and open to public scrutiny
- Creating an environment where research is conducted ethically and where suspected incidents of non-compliant conduct are addressed.

An allegation of research misconduct has been filed with NIST regarding the following: ***Insert as specific and detailed a description of the allegation as possible here, but do not disclose the name or other personally identifiable information of the person(s) who filed the allegation.***

This allegation has not yet been investigated or determined to have merit. However, pursuant to NIST P 5200.00 Responsible Conduct of Research Policy, I will appoint an Inquiry Committee to conduct an inquiry to determine its merits. You must preserve and provide to my office all original research records and materials relevant to the above allegation.

An interview will be scheduled with you to discuss the allegation and will be part of the official record. You may also provide for the record a written response to the allegation. If you choose to provide a written response, it must be submitted to the RCO within 10 business days following your interview date, unless an extension is granted by the RCO based on your written request submitted in advance of that deadline.

Once an inquiry into this matter is concluded, I will inform you in writing that: (1) a review of this matter has dismissed the allegation and the matter is closed; or (2) in the course of the inquiry of this matter, it was determined that further investigation is warranted, and you will be contacted about an investigation phase. If the matter is referred to an Investigation Committee, the Chairperson of the Investigation Committee will notify you of your rights concerning their

review, your obligations during their investigation, and your opportunity to respond to the allegation.

I have attached a copy of the NIST Directives P 5200.00, O 5201.00 and PR 5201.01, on Responsible Conduct of Research. Please review them carefully and let me know if you have any questions about this process.

APPENDIX F

EMPLOYEE INFORMATION AND ACKNOWLEDGMENT FORM

The Chairperson of the Research Misconduct Inquiry Committee will ensure that the respondent of the allegation initials each statement below and returns the original signed/dated form to the Research Conduct Officer. A copy of the completed form will be provided to the respondent of the allegation.

The employee acknowledges that:

I have been informed and I understand this is a formal review and fact-finding process involving matters relating to my official duties as a Federal employee.

I have been informed and I understand that, as a Federal employee, I am required to cooperate with this formal process and provide truthful answers.

I have been informed and I understand that if I refuse to cooperate and answer questions during this formal process, my refusal to cooperate can be a basis for disciplinary action, which may result in my removal from Federal service.

I have been informed and I understand that if I provide information during this formal process that I know to be false at the time I provided the information, my providing false information can be a basis for disciplinary action that may result in my removal from Federal service and also can be a basis for criminal prosecution.

I understand that I will have the opportunity to respond to the allegation and to present evidence to the Inquiry Committee orally and/or in writing and that I may have representation at my own expense.

I understand that I may have rights related to my status as an employee during this process, and that my servicing Human Resources Office can inform me of these rights.

Signature: _____ Date: _____

Name (please print): _____

Position Title, Series and Grade: _____

Duty Station: _____

PRIVACY ACT NOTICE. Pursuant to the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, you are advised of the following:

1. Authority. Solicitation of this information is authorized by 5 U.S.C. 301 that allows the head of an executive department to prescribe regulations for the conduct of its employees and other authorities cited at NIST P 5200.00 and NIST O 5201.00.
2. Principal Purpose. The principal purpose for soliciting the information is to implement NIST P 5200.00 Responsible Conduct of Research Policy.
3. Routine Uses. Routine uses of the solicited information are the same as those listed in the system notice OPM/GOVT-1.
4. Effect of Noncompliance. Failure to provide the solicited information may result in disciplinary action, including the removal from Federal service.

APPENDIX G

ASSOCIATE INFORMATION AND ACKNOWLEDGMENT FORM

The Chairperson of the Research Misconduct Inquiry Committee will ensure that the respondent of the allegation initials each statement below and returns the original signed/dated form to the Research Conduct Officer. A copy of the completed form will be provided to the respondent of the allegation.

The Associate acknowledges that:

I have been informed and I understand this is a formal review and fact-finding process involving matters relating to my official duties as a NIST Associate.

I have been informed and I understand that if I refuse to cooperate and answer questions during this formal process, my refusal to cooperate may result in termination of my Associate agreement.

I have been informed and I understand that if I provide information during this formal process that I know to be false at the time I provide the information; my providing false information can be a basis for termination of my Associate agreement.

I understand that I will have the opportunity to respond to the allegation and to present evidence to the Inquiry Committee orally and/or in writing and that I may have representation at my own expense.

Signature: _____ Date: _____

Name (please print): _____

Office: _____

PRIVACY ACT NOTICE. Pursuant to the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, you are advised of the following:

1. Authority. Solicitation of this information is authorized by 5 U.S.C. 301 that allows the head of an executive department to prescribe regulations for the conduct of its employees and other authorities cited at NIST P 5200.00 and NIST O 5201.00.

2. Principal Purpose. The principal purpose for soliciting the information is to implement NIST P 5200.00 Responsible Conduct of Research Policy.

3. Routine Uses. Routine uses of the solicited information are the same as those listed in the system notice SORN NIST-1.

4. Effect of Noncompliance. Failure to provide the solicited information may result in termination of your Associate agreement.

APPENDIX H

CONFIDENTIALITY AGREEMENT FOR MEMBERS OF AN INQUIRY OR INVESTIGATION COMMITTEE

Acknowledgement of confidentiality of research misconduct inquiry/investigation information.

I agree to treat as confidential all information about claimant, respondents and witnesses that I learn during the performance of my duties on the NIST Research Misconduct Inquiry and/or Investigation Committee regarding the allegation against ____ in regard to _____,

I understand that it would be a violation of NIST P 5200.00 to disclose such information.

As a member of the Inquiry/Investigation Committee, I have been cautioned to demonstrate professionalism, good judgment, and care to avoid unauthorized or inadvertent disclosures of confidential information.

Signature of Research Misconduct Inquiry/Investigation Committee member

Date _____ Name _____

APPENDIX I

PROCEDURE FOR CONDUCTING THE INQUIRY

A. Initiation and Purpose of the Inquiry

Once the RCO determines that the criteria for an inquiry are met, he or she will immediately assign a case number and initiate the inquiry process. The purpose of the inquiry is to conduct an initial review of the available evidence to determine whether to conduct an investigation. An inquiry does not require a full review of all the evidence related to the allegation.

At the time of or before beginning an inquiry, the RCO must make a good faith effort to notify the respondent in writing, if the respondent is known. If the inquiry subsequently identifies additional respondents, they also must be notified in writing.

B. Notice to Respondent; Sequestration of Research Records

On or before the date on which the respondent is notified, or the inquiry begins, whichever is earlier, the RCO must take all reasonable and practical steps to obtain custody of all the research records and evidence needed to conduct the research misconduct proceeding, inventory the records and evidence and sequester them in a secure manner, except that where the research records or evidence encompass scientific instruments shared by a number of users, custody may be limited to copies of the data or evidence on such instruments, so long as those copies are substantially equivalent to the evidentiary value of the instruments.

C. Appointment of the Inquiry Committee and Inquiry Official

The RCO, in consultation with other institutional officials as appropriate, will appoint an Inquiry Committee and eCommittee eChair as soon after the initiation of the inquiry as is practical. The Inquiry Committee Chair will convene all committee meetings and prepare the final report of the committee. The respondent will be notified of the proposed committee membership, and given 10 business days to object to a proposed member based upon a personal, professional, or financial conflict of interest. The RCO makes the final determination of whether a conflict exists.

The RCO shall ensure that those committees are properly staffed and that there is expertise appropriate to carry out a thorough and authoritative evaluation of the evidence.

The RCO shall assign an Inquiry Official to receive and decide on the contents of the inquiry report.

D. Charge to the Committee and First Meeting

The RCO will prepare a charge for the Inquiry Committee that:

- Sets forth the time for completion of the inquiry;
- Describes the allegations and any related issues identified during the allegation assessment;
- States that the purpose of the inquiry is to conduct an initial review of the evidence, including the testimony of the respondent, claimant and key witnesses, and to determine whether an investigation is warranted, not to make a finding with respect to whether research misconduct occurred;
- States that an investigation is warranted if the committee determines:
 - (1) There is a reasonable basis for concluding that the allegation falls within the definition of research misconduct and is within the jurisdictional criteria of NIST P 5200.00 and NIST O 5201.00 (b); and,
 - (2) The allegation may have substance, based on the committee's review during the inquiry.
- Informs the Inquiry Committee that they are responsible for preparing or directing the preparation of a written report of the inquiry that meets the requirements of NIST O 5201.00 and follows the procedure in Appendix J below.

At the committee's first meeting, the RCO will review the charge with the committee, discuss the allegations, any related issues, and the appropriate procedures for conducting the inquiry; assist the committee with organizing plans for the inquiry; and answer any questions raised by the committee. The RCO will be present or available throughout the inquiry to advise the committee as needed and consult with the committee prior to its decision on whether to recommend that an investigation is warranted on the basis of the criteria in the NIST's policies and procedures.

E. Inquiry Process

The Inquiry Committee will normally interview the claimant, the respondent and key witnesses as well as examine relevant research records and materials, or request any information they believe is relevant. Then the Inquiry Committee will evaluate the evidence, including the testimony obtained during the inquiry. After consultation with the RCO, the committee members will decide whether an investigation is warranted based on the criteria in NIST O 5201.00 and:

- (1) A reasonable basis for concluding that the allegation falls within the definition of research misconduct under this directive and involves NIST supported research, research training or activities related to that research or research training; and
- (2) Preliminary information-gathering and preliminary fact-finding from the inquiry indicates that the allegation may have substance.

The RCO shall:

- provide the Inquiry Committee with needed logistical support, e.g., expert advice, including forensic analysis of evidence, and clerical support, including arranging witness interviews and recording or transcribing those interviews, assist the Inquiry Committee in preparing a draft inquiry report,
- send the respondent a full copy of the draft inquiry report and the claimant the portions of the draft report that contain their respective input for comment within a time period that permits the inquiry to be completed within the allotted time,
- take appropriate action to protect the confidentiality of the draft report,
- receive any comments on the draft inquiry report from the respondent and the claimant, and
- ensure that the comments of the respondent and claimant are attached to the final inquiry report.

The scope of the inquiry is not required to and does not normally include deciding whether a finding of research misconduct is warranted. However, if a legally sufficient admission of research misconduct is made by the respondent, misconduct may be determined at the inquiry stage if all relevant issues are resolved. In such cases, Appendix S, T and U can be modified to reflect that sufficient evidence to warrant a finding of research misconduct emerged at the inquiry phase.

F. Time for Completion

The inquiry, including preparation of the final inquiry report and the decision of the IO on whether an investigation is warranted, must be completed within 60 calendar days of initiation of the inquiry, unless the RCO determines that circumstances clearly warrant a longer period. If the RCO approves an extension, the inquiry record must include documentation of the reasons for exceeding the 60-day period. The respondent and claimant will be notified of the extension.

APPENDIX J

PROCEDURE FOR DEVELOPING THE INQUIRY REPORT

A. Elements of the inquiry report

A written inquiry report must be prepared that includes the following information:

- (1) The name and position of the respondent;
- (2) A description of the allegations of research misconduct;
- (3) The case number assigned by the RCO to the allegation.
- (4) The NIST support, including, for example, grant numbers, grant applications, contracts and publications listing NIST support;
- (5) The basis for recommending or not recommending that the allegations warrant an investigation;
- (6) Any comments on the draft report by the respondent or claimant.

NIST's Office of the Chief Counsel shall review the report for legal sufficiency. Modifications should be made as appropriate in consultation with the RCO and the Inquiry Committee prior to release of draft or final reports by the committee. The inquiry report should include: the names and titles of the committee members and experts who conducted the inquiry; a summary of the inquiry process used; a summary of the research records reviewed; summaries of any interviews; and whether any other actions should be taken if an investigation is not recommended.

B. Notification to the Respondent and Claimant and Opportunity to Comment

The RCO shall notify the respondent whether or not the inquiry found an investigation to be warranted, include a copy of the full draft inquiry report, and include a copy of or refer to NIST P 5200.00, NIST O 5201.00 and NIST PR 5201.01.

The RCO shall notify the claimant whether or not the inquiry found an investigation to be warranted, and provide relevant portions of the draft inquiry report to the claimant, and include a copy of or refer to NIST P 5200.00, NIST O 5201.00 and NIST PR 5201.01.

The respondent and claimant shall provide any comments on the draft inquiry report to the RCO within 10 business days of receipt of the draft inquiry report from the RCO.

Any comments that are submitted by the respondent or claimant will be attached to the final inquiry report. Based on the comments, the Inquiry Committee may revise the draft

report as appropriate and prepare it in final form. The committee will deliver the final report to the RCO.

C. NIST Decision and Notification

1. Decision by Inquiry Official

The RCO will transmit the final inquiry report and any comments to the IO, who will determine in writing whether an investigation is warranted. The inquiry is completed when the IO makes this determination.

2. Documentation of Decision Not to Investigate

If the IO decides that an investigation is not warranted, the RCO, with concurrence of NIST's Office of the Chief Counsel, shall secure and maintain, in accord with the NIST records retention policy, sufficiently detailed documentation of the inquiry to permit a later assessment of the reasons why an investigation was not conducted. These documents must be provided to authorized DoC personnel upon request.

APPENDIX K

CLOSURE MEMORANDUM TO RESPONDENT FOLLOWING INQUIRY

TO: Respondent

Through: Supervisor

FROM: NIST Research Conduct Officer

CC: NIST Chief Counsel and Respondent's AD and OU Director

SUBJECT: Resolution of Allegation of Research Misconduct Case #

After an inquiry into the allegation of research misconduct that was filed against you, the Inquiry Official that I appointed to review the Inquiry Committee's findings has found that no further investigation is warranted at this time. ***(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).*** A copy of the final report of the Inquiry Committee is attached to this memorandum. As a result, the inquiry into the concerns reflected in this allegation is considered closed. I appreciate your cooperation in this important process.

Please contact me to discuss steps that can be taken to restore any damage to your reputation that may have arisen as a result of this allegation.

APPENDIX L

CLOSURE MEMORANDUM TO CLAIMANT FOLLOWING INQUIRY

TO: Claimant

FROM: NIST Research Conduct Officer

SUBJECT: Resolution of Allegation of Research Misconduct Case #

After an inquiry into the allegation of research misconduct that you filed against, the Inquiry Official that I appointed to review the Inquiry Committee's findings has found that no further investigation is warranted at this time. *(Insert as specific and detailed a description of the allegation)*. A copy of final report of the Inquiry Committee is attached to this memorandum. As a result, the inquiry into the concerns reflected in this allegation is considered closed. I appreciate your cooperation in this important process.

APPENDIX M

NOTIFICATION TO RESPONDENT OF INVESTIGATION OF ALLEGED RESEARCH MISCONDUCT

TO: Respondent

FROM: Chairperson of the Research Misconduct Investigation Committee

CC: NIST Chief Counsel, NIST Research Conduct Officer, and Respondent's AD, OU Director and Supervisor

SUBJECT: Investigation of alleged research misconduct case #

After an inquiry into the allegation of research misconduct that was filed against you, it has been determined that further investigation into the allegation is warranted.

(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).

You will be contacted shortly about the investigation phase of this process. An interview will be scheduled with you to discuss the allegation and will be part of the official record. You may also provide for the record a written response to the allegation. If you chose to provide a written response, it must be submitted to the NIST Research Conduct Officer within 10 business days following your interview date, unless an extension is granted by the NIST Research Conduct Officer based on your written request submitted in advance of that deadline.

Once the investigation into this matter is concluded, you will be informed in writing that: (1) a review of this matter has dismissed the allegation and the matter is closed; or (2) in the course of the investigation of this matter, there has been a finding of research misconduct and you will be contacted regarding recommended disciplinary steps.

I have attached a copy of the NIST Directives P 5200.00, O 5201.00 and PR 5201.01, on Responsible Conduct of Research. Please review them carefully and let me know if you have any questions about this process.

APPENDIX N

NOTIFICATION TO CLAIMANT OF INVESTIGATION OF ALLEDGED RESEARCH MISCONDUCT

TO: Claimant

FROM: Chairperson of the Research Misconduct Investigation Committee

CC: NIST Research Conduct Officer

SUBJECT: Investigation of alleged research misconduct case #

After an inquiry into the allegation of research misconduct that you filed against, it has been determined that further investigation into the allegation is warranted.

(Insert as specific and detailed a description of the allegation).

You will be contacted shortly about the investigation phase of this process. An interview will be scheduled with you to discuss the allegation and will be part of the official record. You may also provide for the record a written response to the allegation. If you chose to provide a written response, it must be submitted to the NIST Research Conduct Officer within 10 business days following your interview date, unless an extension is granted by the NIST Research Conduct Officer based on your written request submitted in advance of that deadline.

Once the investigation into this matter is concluded, you will be informed in writing that: (1) a review of this matter has dismissed the allegation and the matter is closed; or (2) in the course of the investigation of this matter, there has been a finding of research misconduct.

I have attached a copy of the NIST Directives P 5200.00, O 5201.00 and PR 5201.01, on Responsible Conduct of Research. Please review them carefully and let me know if you have any questions about this process.

APPENDIX O

PROCEDURE FOR CONDUCTING THE INVESTIGATION

A. Initiation and Purpose

The investigation must begin within 30 calendar days after the determination by the IO that an investigation is warranted. The purpose of the investigation is to develop a factual record by exploring the allegations in detail and examining the evidence in depth, leading to recommended findings on whether research misconduct has been committed, by whom, and to what extent. The investigation will also determine whether there are additional instances of possible research misconduct that would justify broadening the scope beyond the initial allegations. This is particularly important where the alleged research misconduct involves clinical trials or potential harm to human subjects or the general public or if it affects research that forms the basis for public policy, clinical practice, or public health practice. Under NIST O 5201.00 the findings of the investigation must be set forth in an investigation report.

On or before the date on which the investigation begins, the RCO must make a good faith effort to notify the respondent in writing of the allegations to be investigated, if the respondent is known. The RCO must also give the respondent written notice of any new allegations of research misconduct within a reasonable amount of time of deciding to pursue allegations not addressed during the inquiry or in the initial notice of the investigation.

B. Sequestration of Research Records

The RCO will, prior to notifying respondent of the allegations, take all reasonable and practical steps to obtain custody of and sequester in a secure manner all research records and evidence needed to conduct the research misconduct proceeding that were not previously sequestered during the inquiry. The need for additional sequestration of records for the investigation may occur for any number of reasons, including NIST's decision to investigate additional allegations not considered during the inquiry stage or the identification of records during the inquiry process that had not been previously secured. The procedures to be followed for sequestration during the investigation are the same procedures that apply during the inquiry.

C. Appointment of the Investigation Committee

The RCO, in consultation with other institutional officials as appropriate, will appoint an Investigation Committee and the Committee Chair as soon after the beginning of the investigation as is practical. The Investigation Committee must consist of individuals who do not have personal, professional, or financial conflicts of interest with those involved with the investigation and should include individuals with the appropriate scientific expertise to evaluate the evidence and issues related to the allegation, interview

the respondent and claimant and conduct the investigation. Individuals appointed to the Investigation Committee may also have served on the Inquiry Committee. When necessary to secure the necessary expertise or to avoid conflicts of interest, the RCO may select committee members from outside NIST, arranging Special Government Employee appointments, if appropriate. The RCO will notify the respondent of the proposed committee membership, and the respondent will have 10 business days to object to a proposed member based upon a personal, professional, or financial conflict of interest. The RCO will make the final determination of whether a conflict exists. All members of the Investigation Committee will be required to sign Confidentiality Agreements regarding the Investigation (Appendix H).

D. Charge to the Investigation Committee and the First Meeting

1. Charge to the Investigation Committee

The RCO will define the subject matter of the investigation in a written charge to the committee that:

- Describes the allegations and related issues identified during the inquiry;
- Identifies the respondent;
- Informs the committee that it must conduct the investigation as prescribed in paragraph E. of this section;
- Defines research misconduct and provides copies of NIST P 5200.00, NIST O 5201.00, NIST PR 5201.01 and any other relevant NIST Directives;
- Informs the committee that it must evaluate the evidence and testimony to determine whether, based on a preponderance of the evidence, research misconduct occurred and, if so, the type and extent of it and who was responsible;
- Informs the committee that in order to determine that the respondent committed research misconduct it must find that a preponderance of the evidence establishes that:
 - (1) Research misconduct, as defined in the NIST policy, occurred (respondent has the burden of proving by a preponderance of the evidence any affirmative defenses raised, including honest error or a difference of opinion);
 - (2) The research misconduct is a significant departure from accepted practices of the relevant research community; and
 - (3) The respondent committed the research misconduct intentionally, knowingly, or recklessly;

- Informs the committee that it must prepare or direct the preparation of a written investigation report that meets the requirements of Appendix P.

2. First Meeting

The RCO will convene the first meeting of the Investigation Committee to review the charge, the inquiry report, and the prescribed procedures and standards for the conduct of the investigation, including the necessity for confidentiality and for developing a specific investigation plan. The RCO will be present or available throughout the investigation to advise the committee as needed.

E. Investigation Process

The Investigation Committee and the RCO must:

- Ensure that the investigation is thorough and documented sufficiently, and includes examination of all research records and evidence relevant to reaching a decision on the merits of each allegation;
- Take reasonable steps to ensure an impartial and unbiased investigation;
- Interview each respondent, claimant, and any other available person who has been reasonably identified as having information regarding any relevant aspects of the investigation, including witnesses identified by the respondent, and record or transcribe each interview, provide the recording or transcript to the interviewee for correction, and include the recording or transcript in the record of the investigation; and
- Pursue diligently all significant issues and leads discovered that are determined relevant to the investigation, including any evidence of any additional instances of possible research misconduct, and continue the investigation to completion.

F. Responsibilities of the RCO during an Investigation

- Provide the Investigation Committee with needed logistical support, e.g., expert advice, including forensic analysis of evidence, and clerical support, including arranging interviews with witnesses and recording or transcribing those interviews.
- Assist the Investigation Committee in preparing a draft investigation report that meets the requirements of Appendix P of this directive.
- Transmit the draft investigation report to NIST Office of the Chief Counsel for a review of its legal sufficiency.
- Sending the respondent and claimant a copy of the draft report for his/her comment and receiving their comments, taking appropriate action to protect the confidentiality

of the draft report, receiving any comments from the respondent and claimant and ensuring that the comments are included and considered in the final investigation report.

- Transmit the final investigation report to the DO and, if the DO determines that further fact-finding or analysis is needed, receive the report back from the DO for that purpose;
- When a final decision on the case is reached, the RCO will normally notify both the respondent and the claimant in writing and will determine whether law enforcement agencies, professional societies, professional licensing boards, editors of affected journals, collaborators of the respondent, or other relevant parties should be notified of the outcome of the case to the best of the RCO's ability.

G. Time for Completion

The investigation is to be completed within 120 calendar days, including conducting the investigation, preparing the report of findings, providing the draft report for comment and sending the final report to the DO. If the RCO determines that the investigation will not be completed within this 120-day period, he/she will submit a written request for an extension to the DO, setting forth the reasons for the delay. The RCO will ensure that periodic progress reports are filed with DO, if the DO grants the request for an extension and directs the filing of such reports.

APPENDIX P

PROCEDURE FOR DEVELOPING THE INVESTIGATION REPORT

A. Elements of the investigation report

The Investigation Committee and the RCO are responsible for preparing a written draft report of the investigation that:

- Describes the nature of the allegation of research misconduct, including identification of the respondent;
- Describes and documents the NIST support, including, for example, the numbers of any grants that are involved, grant applications, contracts, and publications listing NIST support;
- Lists any current support or known applications or proposals for support that the respondent has pending with non-NIST federal agencies;
- Describes the specific allegations of research misconduct considered in the investigation;

Includes the NIST policies, orders, and procedures under which the investigation was conducted;

- Identifies and summarizes the research records and evidence reviewed and identifies any evidence taken into custody but not reviewed;
- Includes a statement of findings for each allegation of research misconduct identified during the investigation. Each statement of findings must:
 - (1) Identify whether the research misconduct was falsification, fabrication, or plagiarism, and whether it was committed intentionally, knowingly, or recklessly;
 - (2) Summarize the facts and the analysis that support the conclusion and consider the merits of any reasonable explanation by the respondent, including any effort by respondent to establish by a preponderance of the evidence that he or she did not engage in research misconduct because of honest error or a difference of opinion;
 - (3) Identify whether any publications need correction or retraction; and
 - (4) Identify the person(s) responsible for the misconduct.
- Has been reviewed by NIST Office of the Chief Counsel prior to distribution beyond the Investigation Committee.

B. Comments on the Draft Report and Access to Evidence

1. Respondent

The RCO must give the respondent a copy of the draft investigation report for comment and, concurrently, a copy of, or supervised access to the evidence on which the report is based. The respondent will be allowed 30 calendar days from the date he/she received the draft report to submit comments to the RCO. The respondent's comments must be included and considered in the final report.

2. Claimant

The RCO must give the claimant a copy of the draft investigation report for comment. The claimant's comments must be submitted to the RCO within 30 calendar days of the date on which he/she received the draft report and the comments must be included and considered in the final report.

3. Confidentiality

In distributing the draft report, or portions thereof, to the respondent, and claimant, the RCO will inform the recipient of the confidentiality under which the draft report is made available and may establish reasonable conditions to ensure such confidentiality.

C. Decision by Deciding Official

The RCO will assist the Investigation Committee in finalizing the draft investigation report, including ensuring that the respondent's and claimant's comments are included and considered, and transmit the final investigation report to the DO, who will determine in writing:

- (1) Whether NIST accepts the investigation report, its findings, and the recommended NIST actions; and
- (2) The appropriate NIST actions in response to the accepted findings of research misconduct.

If this determination varies from the findings of the Investigation Committee, the DO will, as part of his/her written determination, explain in detail the basis for rendering a decision different from the findings of the Investigation Committee. Alternatively, the DO may return the report to the Investigation Committee with a request for further fact-finding or analysis.

When a final decision on the case has been reached, the RCO will normally notify both the respondent and the claimant in writing. The DO will determine whether law enforcement agencies, professional societies, professional licensing boards, editors of affected journals in which falsified reports may have been published, collaborators of the

respondent in the work, or other relevant parties should be notified of the outcome of the case. The RCO is responsible for ensuring compliance with all notification requirements of funding or sponsoring agencies.

D. Appeals

(1) General. Any person adversely affected or aggrieved by a decision by the DO may obtain review by filing, within 90 days after receiving notice of the decision, an administrative appeal to the Director of NIST.

(2) Form of Appeal. An appeal shall be submitted in writing to Director of NIST, 100 Bureau Drive, Gaithersburg, Maryland 20899, and shall include:

The name, street address, email address and telephone number of the person seeking review;

A copy of the decision from which appeal is taken;

A statement of arguments, together with any supporting facts or information, concerning the basis upon which the decision should be reversed; and

A request for hearing of oral argument before the Director, if desired.

(3) Hearing. If requested in the appeal, a date will be set for hearing of oral argument before a representative of the Director of NIST, by the person or the person's designated attorney, and a representative of NIST familiar with the decision from which appeal has been taken. Unless it shall be otherwise ordered before the hearing begins, oral argument will be limited to thirty minutes for each side. A person need not retain an attorney or request an oral hearing to secure full consideration of the facts and the person's arguments.

(4) Decision. After a hearing on the appeal, if a hearing was requested, the Director of NIST shall issue a decision on the matter within 120 days, or, if no hearing was requested, within 90 days of receiving the appeal. The decision of the Director of NIST shall be made after consideration of the arguments and statements of fact and information in the person's appeal, and the hearing of oral argument if a hearing was requested, but the Director of NIST at his or her discretion and with due respect for the rights and convenience of the person and the agency, may call for further statements on specific questions of fact or may request additional evidence in the form of affidavits on specific facts in dispute. After the original decision is issued, an appellant shall have 30 days (or a date as may be set by the Director of NIST before the original period expires) from the date of the decision to request a reconsideration of the matter. The Director's decision becomes final 30 days after being issued, if no request for reconsideration is filed, or on the date of final disposition of a decision on a petition for reconsideration.

E. Confidentiality

Disclosure of the identity of respondents and claimants in appeals is limited, to the extent possible, to those who need to know, consistent with a thorough, competent, objective, and fair proceeding, and in compliance with applicable law.

F. Employee Appeals of Disciplinary Actions

An employee who faces disciplinary proceedings arising from an allegation of research misconduct has available a number of established procedures providing for the employee's rights to appeal or otherwise challenge a disciplinary matter. These may include rights under the Merit Systems Protection Board regulations, Equal Employment Opportunity Commission (EEOC) regulations, and grievance procedures.

G. Maintaining Records for Review

The RCO must maintain “records of research misconduct proceedings” following the NIST Comprehensive Records Schedule.

APPENDIX Q

CLOSURE MEMORANDUM TO RESPONDENT FOLLOWING INVESTIGATION

TO: Respondent

Through: Supervisor

FROM: NIST Research Conduct Officer

CC: NIST Chief Counsel and Respondent's AD and OU Director

SUBJECT: Resolution of Allegation of Research Misconduct case #

After an investigation into the allegation of research misconduct that was filed against you, the Deciding Official for NIST research misconduct cases has found the evidence does not support a finding of research misconduct. ***(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation)***. A copy of the final report of the Investigation Committee is attached to this memorandum. As a result, the investigation into the concerns reflected in this allegation is considered closed. I appreciate your cooperation in this important process.

Please contact me to discuss steps that can be taken to restore any damage to your reputation that may have arisen as a result of this allegation.

APPENDIX R

CLOSURE MEMORANDUM TO CLAIMANT FOLLOWING INVESTIGATION

TO: Claimant

FROM: NIST Research Conduct Officer

SUBJECT: Resolution of Allegation of Research Misconduct case #

After an investigation into the allegation of research misconduct that you filed against, the Deciding Official for NIST research misconduct cases has found the evidence does not support a finding of research misconduct to be without merit. ***(Insert as specific and detailed a description of the allegation)***. A copy of the final report of the Investigation Committee is attached to this memorandum. As a result, the inquiry into the concerns reflected in this allegation is considered closed. I appreciate your cooperation in this important process.

APPENDIX S

RESEARCH MISCONDUCT FINDING MEMORANDUM TO THE RESPONDENT

TO: Respondent

Through: Supervisor

FROM: NIST Research Conduct Officer

CC: NIST Chief Counsel and Respondent's AD and OU Director

SUBJECT: Resolution of Allegation of Research Misconduct case #

In the course of an investigation into the allegation of research misconduct that was filed against you, the Deciding Official for NIST research misconduct has found that the preponderance of the evidence supports the charge.

(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).

The attached Investigation Report provides a detailed description of the findings.

Disciplinary actions recommended...

APPENDIX T

RESEARCH MISCONDUCT FINDING MEMORANDUM TO THE CLAIMANT

TO: Claimant

FROM: NIST Research Conduct Officer

SUBJECT: Resolution of Allegation of Research Misconduct case #

I am informing you that, in the course of an investigation into the allegation of research misconduct that you filed against, the Deciding Official for NIST research misconduct cases has found that the preponderance of the evidence supports the charge.

(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).

Disciplinary actions recommended...

APPENDIX U

RESEARCH MISCONDUCT MEMORANDUM TO THE NIST ASSOCIATE DIRECTOR FOR LABORATORY PROGRAMS

TO: NIST Associate Director of Laboratory Programs

FROM: NIST Research Conduct Officer

CC: NIST Chief Counsel and Respondent's OU Director and Supervisor

SUBJECT: Research Misconduct case #

I am informing you that, in the course of an investigation into the allegation of research misconduct that was filed against, I have found that the preponderance of the evidence supports the charge. *(Insert as specific and detailed a description of the allegation as possible but do not disclose the name or other personally identifiable information of the person who filed the allegation).*

As a result, it is recommended that NIST management pursue administrative actions commensurate with the severity *(insert a brief summary of the implications of this violation, being clear to address intent)*

It is also recommended that NIST management take immediate steps to address the impact created by the actions of the respondent. *(Include specific steps to publicly address the effects of the misconduct and to the identify the respondent in a manner that will prevent future occurrences)*

APPENDIX V

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	11 June 12	Richard Cavanagh(OSP)	First Draft
Draft	2014	Nicholas Barbosa	Vetted by team
		Timothy Burns	
		Richard Cavanagh	
		Michael H. Kelley	
		Michael Moore	
		Sheila Nichols	
		Henry Wixon	
		David Yashar	
		Nikolai Zhitenev	
Ver .01	11/19/2014	Dan Cipra	Incorporated DRB Comments

Participation in Documentary Standards Activities

NIST P 5300.00
Effective Date: 8/15/2012

PURPOSE

Establish the National Institute of Standards and Technology (NIST) Policy on Participation in Documentary Standards Activities

SCOPE

All NIST employees and contractors engaged in documentary standards activities for NIST.

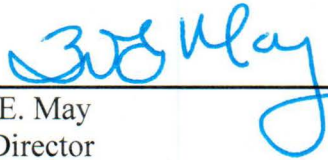
LEGAL AUTHORITY AND REFERENCES

- [Public Law 104-113, National Technology Transfer and Advancement Act of 1995](#), Section 12(d), as amended by Section 1115 of [Public Law 107-107](#)
- OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, January 27, 2016:
 - [Federal Register Notice](#)
 - [Direct link](#) to Revised (2016) OMB Circular A-119
- [Memorandum for the Heads of Executive Departments and Agencies, Principles for Federal Engagement in Standards Activities to Address National Priorities, issued by OMB, USTR, and OSTP](#) January 17, 2012

POLICY

It is NIST policy to encourage staff participation in domestic and international standards body activities, whenever such participation is in the public interest and is compatible with NIST's mission, policies, positions, priorities and available resources. NIST's engagement in documentary standards activities is an important means by which NIST transfers knowledge to the private sector, to accelerate technology development and accomplish its mission of promoting U.S. innovation and industrial competitiveness. Only NIST employees and contractors, contracted for that purpose, may participate in a standards body on NIST's behalf.

The Associate Director for Laboratory Programs is responsible for ensuring that processes and procedures are developed, implemented and maintained that encourage individual and organizational responsibility in engagement in the development and application of documentary standards on behalf of NIST.



Willie.E. May
NIST Director

JUL 06 2016

Date

Participation in Documentary Standards Activities

NIST O 5301.00

Effective Date: 10/11/2012

PURPOSE

This directive describes the requirements and responsibilities for the acceptance and maintenance of memberships on government and nongovernment standards bodies working in areas related to the activities of the National Institute of Standards and Technology (NIST).

APPLICABILITY

This issuance is applicable to all NIST employees and contractors, contracted for that purpose, who participate in standards activities conducted by or on behalf of NIST.

REFERENCES

- [OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities](#), dated January 27, 2016
- [Guidelines for NIST Staff Participating in Documentary Standards Developing Organizations' Activities \(NISTIR 7854\)](#)
- [P 5300.00 Participation in Documentary Standards Activities](#)

PRINCIPLES AND REQUIREMENTS

NIST manages its documentary standards activities strategically by setting priorities for standards activities appropriate to the overall NIST mission and by allocating staff resources effectively. NIST values participation in standards activities and provides mechanisms for recognition of effective activity. NIST engagement in documentary standards activities is guided by five fundamental strategic objectives:

- Ensure timely availability of effective standards and efficient conformity assessment schemes critical to addressing identified NIST priorities, including national priorities established in statute or Administration policy;
- Achieve cost-efficient, timely and effective solutions to legitimate regulatory, procurement and policy objectives;
- Promote standards and standardization systems that enable innovation and foster competition;
- Enhance U.S. competitiveness while ensuring national treatment¹; and
- Facilitate international trade and avoid the creation of unnecessary obstacles to trade.

¹ National treatment is the principle of giving others the same treatment as one's own nationals.
(http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm)

In order to realize these objectives, NIST works with the private sector to address common standards needs, looking to private sector standards development processes that are well coordinated, open, deliver optimal outcomes for all stakeholders and are internationally accepted.

In accordance with *OMB Circular A-119*, participation in an organization or body does not necessarily connote NIST agreement with, or endorsement of, the decisions reached by the organization or body or the standards developed by standards bodies.

DEFINITIONS

Board - the governing body of an organization such as an incorporated firm or nonprofit. The board, having ultimate decision-making authority, is empowered to set policy, adopt bylaws, and perform other tasks required for governance. It may hold a fiduciary capacity and may be held liable for the organization's actions.

Body - Any institute, board, commission, council, conference, panel, task force, committee, or other similar group or organization, or any subcommittee or other subgroup thereof.

Government Liaison – In the role of government liaison, a NIST employee serves as NIST's representative to an outside organization in a non-voting, non-fiduciary capacity. Such service is appropriate where there is need for an exchange of nonproprietary information, or where the service facilitates the coordination of NIST's and the organization's activities.

Individual Membership – Refers to professional affiliation and membership of a NIST employee on external committees/organizations and technical working groups (TWGs), the objectives and outputs of which contribute to the enhancement of the Institute's functions and activities.

Institutional Membership – Refers to institutional professional affiliation and membership of NIST on external committees/organizations and TWGs, the objectives and outputs of which contribute to the enhancement of the Institute's functions and activities.

List of Approved Standards Bodies – A list of standards bodies for which the NIST Director has authorized NIST to pay for memberships.

Policy Making Group - A group within an organization that formulates basic principles and associated guidelines to direct and limit the organization's actions in pursuit of long-term goals.

Standard - The term "standard" includes all of the following:

- (1) Common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices.
- (2) The definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

(3) A set of rules that specify the minimum acceptable level of safety for constructed objects such as buildings and nonbuilding structures, or the safe installation of equipment in structures.

Standards Body - Any governmental or private sector group that exercises policy control over standards activities, or that administers one or more standards programs, or that develops or approves or promulgates standards. Examples of types of standards bodies are treaty organizations where governments are members, such as International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) or Codex Alimentarius; private, voluntary organizations where the United States is represented by a single “national body” organization, such as International Organization for Standardization (ISO) or International Electrotechnical Commission (IEC) where the United States is represented by the American National Standards Institute (ANSI); professional and technical organizations whose membership is on an individual or organizational basis, such as ASTM International or Institute of Electrical and Electronics Engineers (IEEE); and consortia, whose membership is typically technology-based, such as the Cloud Printing Alliance.

RESPONSIBILITIES

NIST Director

- Sets NIST documentary standards participation policy

NIST Associate Director for Laboratory Programs

- Ensures effective implementation of NIST documentary standards policy.
- With support from the Director, Standards Coordination Office (SCO), conducts periodic reviews of the effectiveness of NIST participation in documentary standards activities.
- Ensures effective integration of documentary standards into NIST programmatic priorities and activities, particularly those with involvement of multiple operating units (OUs).

NIST SCO Director

- As authorized by the NIST Director, determines suitability of additions to the NIST List of Approved Standards Bodies.
- Reviews and provides policy guidance on all invitations to serve on boards or policy making bodies of standards bodies.
- Working with NIST OUs, provides leadership and support to facilitate more effective coordination of the standards and conformity assessment activities of the federal, the state and local governments, and the private sector.
- Maintains and promotes the Standards Committee Participation Database (SCPD).
- Annually queries OUs for updates to the SCPD

Chief Counsel for NIST

- Reviews organizational documentation associated with all initial NIST requests for membership in standards bodies.

- After addressing any changes necessary to ensure legal compliance, forwards all approved requests to the Director, SCO.

NIST Management (OU Directors, OU Deputy Directors, and Division Chiefs)

- Include standards activities within overall strategic planning and track progress in NIST program reviews. Explicitly link standards activities to the NIST and OU mission and set priorities accordingly. This includes deliberate selection of committee work that is most likely to result in standards used worldwide, and developing continuity plans for ensuring effective NIST participation in key documentary standards activities.
- Cultivate staff participation in the development and use of pertinent, standards as a key means of transferring NIST technology and research results, and allocate personnel and resources for these activities during the normal planning process.
- Periodically review standards activities to identify gaps in representation for mission-critical areas as part of long range planning.
- Determine appropriateness of staff participation in standards bodies.
- Ensure that staff participation in standards activities is effective and has a measurable and demonstrable impact, and that positive impact is rewarded as appropriate.
- Annually review OU/Division standards participation as documented in the SCPD and update SCO on standards bodies in which they will no longer maintain memberships.

Contracting Officer Representative (COR)

- As delegated by the cognizant Contracting Officer, provide appropriate oversight of contractor performance, where relevant, by requiring timely and periodic reports and meetings.

NIST Employees

- When approved, serve as the NIST principal representative to a standards body.
- Know and act in conformity with established policies and program objectives of NIST, the Department of Commerce, and the Administration, recognizing that for NIST employees who participate in activities related to the professional basis of their employment carry an inseparable identification with NIST.
- Ensure that their participation in standards activities is effective and has a measurable and demonstrable impact.
- Clear with DOC Ethics Division all invitations to serve on boards or policy making bodies of standards bodies approved for NIST membership.
- Record standards participation in the [Standards Committee Participation Database](#) (SCPD)
- Follow *Guidelines for NIST Staff Participating in Voluntary Standards Developing Organizations' Activities* (NISTIR 7854).

When assigned, develop statement of work defining appropriate contractor activities in standards developing committees. Additional guidance can be found in *Guidelines for*

NIST MEMBERSHIP IN STANDARDS BODIES

For All Standards Body Assignments (Committee Participation) –

Committee participation and fee payment must be approved in advance of NIST employees and contractors registering committee membership in the [Standards Committee Participation Database](#). Committee participation must be updated in the SCPD at least annually.

Fees for Standards Bodies –

NIST employee membership fees for standards bodies may be paid by NIST only to entities currently on the List of Approved Standards Bodies. OUs are responsible for paying applicable fees for standards body activities directly to the bodies concerned after obtaining all required approvals except with regard to administrative service fees to ANSI (see below).

Institutional membership (also referred to as "organizational" or "sustaining" membership) is preferred, whenever possible, over individual membership. NIST institutional membership does not confer any individual membership rights or privileges to any member of the NIST staff, including officially designated representatives to the standards body. For approved institutional memberships, NIST OUs may pay using NIST appropriated funds (STRS), reimbursable funds transferred to NIST by a requesting organization for this purpose (membership fees or work with the standards body must be called out in the agreement statement of work), or funds generated by overhead.

NIST payment for an individual membership is only permitted if the standards body does not itself provide for institutional memberships. For approved individual memberships, NIST OUs may pay using NIST appropriated funds (STRS), reimbursable funds transferred to NIST by a requesting organization for this purpose (membership fees or work with the standards body must be called out in the agreement statement of work), or funds generated by overhead. Individual membership fees may be paid either as a membership or indirectly (e.g., where purchase of a society journal would confer membership status on an individual) to standards bodies.

(1) Requests for NIST Payment of Memberships in Bodies Not on the List of Approved Standards Bodies - Requests for approval of membership payment for standards bodies not on the List of Approved Standards Bodies must be sent to the SCO Director for policy determination. The request should be in the form of a memo cleared by the division and signed by the OU Director or designated management, addressed to the SCO Director. The charter and bylaws of the organization and any other relevant documentation (for example, membership application or membership agreement) should be attached to this memo. The SCO Director will make a policy determination and, if the determination is positive, will forward the request to the Chief Counsel for NIST for legal review. The Chief Counsel for NIST will review the organizational documentation and related information to determine whether NIST membership is

legally permissible. The SCO Director forwards all findings to the requestor and OU Director for noting and to Standards Services for listing.

(2) Standards Bodies Administrative Service Fees - Fees may be paid to private sector standards bodies to help cover the costs associated with standards committee operations and communication, including preparation and distribution of minutes, circulation of draft standards, meeting arrangements, and committee records. These fees may be paid to a standards body if required for a NIST unit to serve on one or more committees of that body and if the OU Director or designee determines that the intended committee service is consonant with NIST goals and objectives.

Payment of administrative service fees does not confer individual membership rights or privileges to any member of the NIST staff, nor does it result in NIST becoming an institutional member of the standards body.

OUs must incorporate the following language into all contracts and agreements, relating to the payment of administrative service fees:

"Our payment of these administrative service fees is based on the understanding that:

- (1) The fees will be used exclusively to help cover costs associated with standards committee operation and communication, e.g., preparation and distribution of minutes, circulation of drafts for comment, meeting arrangements, maintenance of committee records, and allocation of dues to international standards development organizations;*
- (2) Payment of administrative service fees to a standards body does not signify that NIST endorses or supports positions taken by that body on any subject or issue; and*
- (3) Payment of the fees does not confer individual membership rights or privileges on any member of the NIST staff nor result in NIST being recognized as an institutional member of (add name of standards body)."*

ANSI charges an administrative service fee in connection with sponsorship of secretariats of committees of international organizations of which ANSI is the recognized U.S. member body. NIST laboratories that sponsor secretariats should determine their fees with ANSI. ANSI annually submits an invoice to SCO covering all NIST international secretariat fees. After reviewing for completeness and accuracy, SCO informs each responsible unit of the portion it must pay. To permit thorough and accurate review, SCO should be provided with copies of all pertinent correspondence and contracts with ANSI regarding administrative service fees. SCO is responsible for forwarding these administrative fees along with the annual institutional membership fee to ANSI.

DIRECTIVE OWNER

601 –Standards Coordination Office

APPENDICES

A – Revision History

Appendix A

Revision History

Revision	Date	Responsible Person	Description of Change
Rev. 2-1.0	5/9/2016	Nathalie Rioux	Version 2 revisions

Measurement Quality

NIST P 5400.00

Effective Date: 11/20/2012

PURPOSE

The purpose of this policy is to maintain and ensure the quality of NIST's measurement services.

SCOPE

This policy applies to all NIST employees involved in the provision of NIST measurement services (calibrations and reference materials) provided to customers both internal and external to NIST.

LEGAL AUTHORITIES AND REFERENCES

- [15 U.S.C. 272](#)(b) and (c).
- Section 504 of the Foreign Relations Authorization Act 1979, codified at [22 U.S.C. 2656d](#)(a).
- *Mutual recognition of national measurement standards and of calibration and measurement certificates issued by national metrology institutes.* [CIPM MRA](#), 14 October 1999. Technical Supplement revised in October 2003 (pages 38-41).
- *NIST Quality Manual for Measurement Services*, [NIST QM-I](#).
- *Department Organizational Order (DOO) 30-2A [contains NIST's statutory and delegated authorities and functions]*.
- [DOO 30-2B \[prescribes the organization and assignment of functions within NIST\]](#).

POLICY

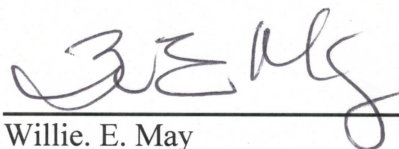
NIST will provide measurement services (including *calibrations* and *certified reference materials*) and measurement results (including those produced in the context of *key comparisons* and other interlaboratory studies) that meet the needs of its customers, satisfy NIST's mission, and fulfill its responsibilities as a global leader in measurements and standards;

NIST will maintain and document the quality of NIST measurement services and of NIST measurement results by means of a quality management system described in the NIST Quality Manual;

NIST will rely on the commitment of all NIST employees whose activities affect the quality of our measurements services to implement the NIST quality management system in their work; and

To the extent permitted by law, NIST maintains a quality management system that conforms with the international standard ISO/IEC 17025 and the relevant requirements of ISO Guide 34 as they apply to the **Standard Reference Materials® (SRMs®)** and related services that NIST delivers.

The Associate Director for Laboratory Programs is responsible for ensuring that requirements, processes, and procedures are developed, implemented, and maintained that guarantee the quality of all NIST measurement services and results, and the NIST Quality Manager is responsible for the implementation, administration, and fulfillment of the reporting requirements for the NIST Quality System.



Willie. E. May
Director

7/24/15
Date

Human Subjects Protections

NIST P 5500.00

Effective Date: 11/24/2014

PURPOSE

To articulate NIST's commitment to protect the rights and safeguard the welfare of human subjects who participate in research conducted or supported by NIST in accordance with the principles stated in the Belmont Report and in compliance with U.S. Federal Regulations that protect Human Subjects (15 CFR Part 27 and 45 CFR Part 46, Subparts B, C and D, when applicable).

SCOPE

This directive applies to all NIST employees and associates conducting scientific research involving human subjects at or for NIST, to the extent allowed by law and the terms of the associate's agreement and all research supported by NIST including work performed at any and all NIST satellite sites.

LEGAL AUTHORITY AND REFERENCES

- The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, (1978). 44 Fed. Reg. 23192 (Apr. 18, 1979).
- 15 CFR Part 27, the Department of Commerce implementation of the Common Rule for Protection of Human Subjects.
- 45 CFR Part 46, Subparts B, C and D, when applicable, Basic HHS Policy for Protection of Human Subjects
- 21 U.S.C. §301 et seq., the Federal Food, Drug and Cosmetics Act, as amended.
- 21 CFR Part 56, Food and Drug Administration (FDA), Institutional Review Boards
- 21 CFR 312, FDA Investigational New Drug Application
- 21 CFR 812, FDA Investigation New Device Exemption

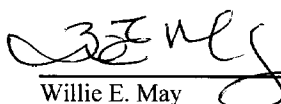
POLICY

In order to protect the rights and well-being of any human subjects participating in research conducted or supported by NIST, it shall be the policy of NIST that all research involving human subjects shall be carried out in accordance with 15 CFR Part 27, the Department of Commerce's

implementation of the Common Rule for Protection of Human Subjects. Under this policy, NIST will ensure that:

- All NIST research involving human subjects is performed according to the highest scientific and ethical standards in a manner that promotes and respects the rights and welfare of all human subjects consistent with all applicable laws, regulations and policies.
- All NIST employees complete training in human research protections that is relevant to their role. Training includes the regulatory definition of research involving human subjects so that NIST employees will recognize or identify such research plans and take necessary steps to obtain appropriate approval before beginning such work.
- NIST continues to maintain an Institutional Review Board (IRB) that exercises independent authority and decision making through prospective and continuing review and approval of non-exempt research involving human subjects in accordance with 15 CFR Part 27.
- NIST establishes and maintains a Human Subjects Protection Office (HSPO) that shall be responsible for overseeing activities related to the NIST Human Subjects Protection Program. HSPO human subject protection experts will provide assistance to NIST employees and review specific cases in a timely and transparent manner.
- Organizational Units (OUs) review all OU-supported research potentially involving human subjects for scientific merit and prepare documentation required under NIST O 5501.00.
- When appropriate, NIST may agree to rely on external IRBs to provide required certifications for research conducted or supported by NIST.

This policy does not affect any state or local laws or regulations which may otherwise be applicable and which provide additional protections for human subjects.



Willie E. May
Director

02 Sept. 2015

Date

NIST Human Subjects Protection Program

NIST O 5501.00
Effective Date: 07/23/2015

PURPOSE

Combined with the NIST Institutional Review Board (IRB) Charter and Human Subjects Protection Office (HSPO) procedures, define the scope and structure of the NIST Human Subjects Protection Program (HSPP) necessary for the effective implementation of NIST P 5500.00, Human Subjects Protections (HSP), and the establishment of the roles and responsibilities of NIST employees and associates conducting scientific research involving human subjects at or for NIST, to the extent allowed by law and the terms of the associate's agreement.

SCOPE

The scope of the NIST HSPP comprises NIST P 5500.00 Human Subjects Protections, this order, the NIST IRB Charter, and the directives, deployment tools, and procedures necessary to implement this order.

APPLICABILITY

This directive applies to all research conducted or supported by NIST.

LEGAL AUTHORITIES AND REFERENCES

- [15 CFR Part 27](#), the Department of Commerce implementation of the Common Rule for Protection of Human Subjects.
- [45 CFR Part 46](#), Subparts B, C and D, when applicable, Basic HHS Policy for Protection of Human Subjects
- 21 U.S.C. §301 et seq., the Federal Food, Drug and Cosmetics Act, as amended.
- 21 CFR Part 56, Food and Drug Administration (FDA), Institutional Review Boards
- 21 CFR 312, FDA Investigational New Drug Application
- 21 CFR 812, FDA Investigation New Device Exemption
- NIST P 5500.00, Human Subjects Protections
- [The Belmont Report](#): Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, (1978). 44 Fed. Reg. 23192 (Apr. 18, 1979).
- NIST Institutional Review Board (IRB) Charter

REQUIREMENTS

NIST shall comply with U.S. Federal Regulations that protect Human Subjects (15 CFR Part 27 and 45 CFR Part 46 Subparts B, C and D).

DEFINITIONS

Certification – means the official notification by the institution to the supporting department or agency, in accordance with the requirements of 15 CFR Part 27, that a research project or activity involving human subjects has been reviewed and approved by an Institutional Review Board (IRB) in accordance with an approved assurance.

Human subject - means a living individual about whom an investigator (whether professional or student) conducting research obtains

- (1) Data through intervention or interaction with the individual, or
- (2) Identifiable private information.

Institution - means any public or private entity or agency (including federal, state, and other agencies).

Intervention - includes both physical procedures by which data are gathered (for example, venipuncture) and manipulations of the subject or the subject's environment that are performed for research purposes.

Interaction - includes communication or interpersonal contact between investigator and subject.

IRB - means an institutional review board established in accord with and for the purposes expressed in 15 CFR Part 27.

IRB approval - means the determination of the IRB that the research has been reviewed and may be conducted at an institution within the constraints set forth by the IRB and by other institutional and federal requirements.

Legally authorized representative - means an individual or judicial or other body authorized under applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure(s) involved in the research.

Minimal risk - means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

Principal Investigator - means the scientist or engineer responsible for the conduct of a defined scope of work or research.

Private information - includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record).

Private information must be individually identifiable (*i.e.*, the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.

Research - means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes. For example, some demonstration and service programs may include research activities.

Research conducted by NIST – means research performed or engaged in by NIST employees.

Research supported by NIST - includes research performed by NIST contractors and NIST funding recipients and may include tangible activities or resources of foreign and domestic guest researchers under their agreements with NIST, activities carried out jointly by NIST and other parties in shared facilities such as the Institute for Bioscience and Biotechnology Research (IBBR) and JILA, and activities performed under CRADAs.

Research subject to regulation - and similar terms are intended to encompass those research activities for which a federal department or agency has specific responsibility for regulating as a research activity, (for example, Investigational New Drug requirements administered by the Food and Drug Administration). It does not include research activities which are incidentally regulated by a federal department or agency solely as part of the department's or agency's broader responsibility to regulate certain types of activities whether research or non-research in nature (for example, Wage and Hour requirements administered by the Department of Labor).

Research team – means a group of two or more NIST employees or non-employees operating in a coordinated or cooperative manner in the interest of a common research goal.

Supported - means to have promoted the interests or cause of various research activities or endeavors through funding, or direct engagement of personnel on the research activity.

ACRONYMS

ADLP – Associate Director of Laboratory Programs

AMD – Acquisition Management Division

CFR – Code of Federal Regulations

CO – Contracting Officer

COR – Contracting Officer's Representative

COS—Chief of Staff

CRADA – Cooperative Research and Development Agreement

FDA – Food and Drug Administration

FPO – Federal Program Officer

FWA – Federalwide Assurance

GMD – Grants Management Division

GO – Grants Officer

HHS – United States Department of Health and Human Services

HSPO – Human Subjects Protections Office

HSPP – Human Subjects Protections Program

IRB – Institutional Review Board

NIST IRB – NIST Institutional Review Board

OAAM – Office of Acquisition and Agreements Management

OHRP – Department of Health and Human Services Office for Human Research Protections

OU – Organizational Unit

PI – Principal Investigator

RESPONSIBILITIES

NIST Director

- Defines and authorizes NIST’s Human Subjects Protection policy in accordance with NIST P 5500.00, 15 CFR Part 27.
- Takes ultimate responsibility for the creation and implementation of the NIST HSPP, ensures the availability of resources required for implementation, and completes required training.
- Serves as the Institutional Official (IO) and is the signatory of the NIST Federalwide Assurance.
- Defines roles, allocates responsibilities and accountabilities, and delegates authorities to ensure that:
 - All NIST research involving human subjects is performed according to the highest scientific and ethical standards in a manner that promotes and respects the rights and welfare of all human subjects consistent with all applicable laws, regulations and policies.
 - All NIST employees complete training in human subjects research protections that is relevant to their role. At a minimum, training includes the regulatory definition of research with human subjects so that NIST personnel may recognize or identify when conducting or supporting such research is appropriate and take necessary steps to gain the required approvals before beginning such work.

- NIST continues to maintain an Institutional Review Board (IRB) that shall be responsible for the prospective and continuing review and approval of research activities conducted by NIST Federal employees involving human subjects in accordance with 15 CFR Part 27.
- NIST establishes and maintains a Human Subjects Protection Office (HSPO) that shall be responsible for overseeing the activities related to the NIST human subjects research portfolio and the maintenance of the NIST Federalwide Assurance (FWA), including the establishment of written policies and procedures required to implement the HSPP.
- Determinations of whether or not research involves human subjects and whether or not research meets the criteria for exemption from IRB review or qualify as not engaged in non-exempt research are made in a timely and transparent manner.
- Organizational Units (OUs) review all OU-supported research potentially involving human subjects for scientific merit and prepare all necessary documentation to inform the determination of whether the proposed research requires review and approval by the NIST IRB.
- When appropriate, NIST may agree to rely on external IRBs to provide required certifications for research conducted or supported by NIST.
- The NIST IRB exercises independent authority and decision making with respect to the review and approval of research with human subjects.
- Ensures that OUs stop work when there are concerns related to the protection of human subjects or when there are concerns of non-compliance with existing requirements.

Associate Director for Laboratory Programs

- Develops appropriate processes and procedures with the ADII and ADMR to ensure that the NIST intramural research and extramural programs (e.g., grants and contracts) satisfy this order, and follow the processes and procedures necessary for the full and effective implementation of the NIST HSPP.
- Supports the NIST Director in the implementation of NIST P 5500.00 Human Subjects Protection.
- Serves as the IO in the absence of or as designated by the NIST Director.
- Ensures that the NIST laboratory programs adhere to the NIST HSPP policy through the implementation of Human Subjects Research related performance criteria for all Laboratory management and supervisory positions.
- Ensures OU process for making determinations on whether work is research, and whether work is research involving human subjects is in accordance with all NIST policies.

- Ensures that OUs stop work/research when there are concerns related to the protection of human subjects, or when there are concerns related to non-compliance with existing requirements.
- Completes required training.

Chief of Staff

- Supports the NIST Director in the implementation of NIST P 5500.00 Human Subjects Protection.
- Raises any concerns associated with research that OUs are performing related to the protection of human subjects, or when there are concerns related to non-compliance with existing requirements to the attention of the Director.
- Completes required training.
- Oversees the functioning of the Human Subjects Protection Office (HSPO).

Organizational Unit Director

- Ensures OU compliance with NIST HSPP policies and procedures.
- Ensures training is completed for all OU staff relevant to their role and makes OU-specific training available when appropriate.
- Completes required training.
- Approves start of research after HSPO determination that the proposed project is: (1) research; (2) human subjects research; (3) exempt human subjects research; and/or (4) non-engagement in non-exempt research, or approves start or continuation of research that has been approved by the HSPO or NIST IRB, either as a new case or after continuing review.
- Facilitates and encourages access to HSPO human subject research protection experts to work with and support PIs in the laboratory programs.
- Ensures any adverse events or unanticipated problems involving risks to subjects or others or any serious or continuing non-compliance occurring from NIST supported or conducted research involving human subjects are reported immediately to appropriate offices including the NIST IRB and HSPO and issues the stop work order with the concurrence of the HSPO Director.
- Ensures that the OU's portfolio of ongoing work/research is monitored to identify potential human subject safety concerns, deviations from approved protocols, or non-compliance with existing requirements, and should such issues occur, stops the active research program.

- Ensures that stoppages of research involving human subjects are reported to the NIST IRB Chair, the HSPO and, if appropriate, the responsible Contract Officer (CO) or Grants Officer (GO).
- Supports any audits and reviews by OHRP or HSPO, or other agencies (e.g. DOD).

Director, Office of Acquisition and Awards Management

- Ensures OAAM compliance with NIST HSPP policies and procedures.
- Completes required training.
- Ensures all OAAM staff complete training relevant to their role.
- Through the responsible CO or GO, verifies that appropriate human subjects-related documentation is approved before research involving human subjects through a grant or contract begins.
- Through the responsible CO or GO, monitors research involving human subjects to ensure compliance with grant or contract terms and conditions.
- Ensures any adverse events or unanticipated problems involving risks to subjects or others, or any serious or continuing noncompliance, occurring from NIST supported or conducted research involving human subjects are reported immediately to appropriate offices including the HSPO.
- Ensures that responsible CO or GO issues a stop work order to contractor or financial assistance recipient in the event of any adverse events or unanticipated problems involving risks to subjects or others, or any serious or continuing noncompliance, occurring from NIST supported or conducted research involving human subjects.
- Ensures that any stoppages of research involving human subjects supported under NIST grants or contracts are reported to the HSPO.

Director, NIST Technology Partnerships Office

- Completes required training and ensures that TPO staff complete any required training.
- Verifies receipt of appropriate human subject protections documentation before agreements (e.g., CRADAs, MTAs etc.) are executed and works with the HSPO to resolve any questions.

Division Chief or organizational equivalent

- Ensures division compliance with NIST HSPP policies and procedures.
- Completes required training and ensures that division employees receive and complete training, and if necessary, provide division-specific training.

- Reviews proposed work/research for scientific merit, feasibility, and support (*i.e.*, external funding, involvement of NIST associates, etc.) and determines whether further review and consultation (*e.g.*, from the HSPO) is necessary.
- Provides timely communication of all findings related to the Human Subjects Research Determination Form to relevant researchers.
- Verifies that OU Director has approved the start of research after HSPO determination that the proposed project is: (1) research; (2) human subjects research; (3) exempt human subjects research; and/or (4) non-engagement in non-exempt research, or that OU Director approved the start or continuation of research after by the HSPO or NIST IRB, either as a new case or after continuing review.
- Ensures that the Division's portfolio of ongoing work/research is monitored to identify unanticipated potential for human subjects safety concerns, deviations from approved protocols, or potential serious or ongoing non-compliance with existing requirements, and should such issues occur, stop the active research program and initiate consultation with HSPO.
- If the proposed work/research is to be performed by contract or grant, ensures that the potential human subject research is identified in the package submitted to AMD/GMD.
- If the work/research is being performed by a contractor or grant recipient, ensures that the CO or GO is notified immediately of any adverse events or unanticipated problems involving risks to subjects or others or any serious or continuing noncompliance. Initiates the process to issue a formal stop work order if appropriate. In addition, ensures that the HSPO is provided the complete IRB package in order to conduct the institutional review annually.
- Ensures that stoppages of work/research involving human subjects are reported to the NIST IRB Chair, the HSPO and, if appropriate, the responsible CO or GO.

Group Leader or organizational equivalent

- Ensures group compliance with NIST HSPP policies and procedures.
- Ensures group staff receive and complete training, and provide group-specific training when necessary.
- Communicates with Division Chief, or equivalent, when proposed work/research might involve human subjects.
- Reviews proposed work/research for scientific merit, feasibility, and support (funding etc.) and determines whether further review and approval (*e.g.*, from the HSPO) is necessary.
- Works with PI to prepare: (1) an adequately detailed Human Subjects Research Determination Form to request a determination from the HSPO Director regarding whether a project is a) research, b) research involving human subjects, c) exempt

human subjects research and/or d) non-engagement in research involving human subjects; (2) an adequately detailed Human Research Protocol and all other related required documents; or (3) a request for continuing review.

- Ensures that no research involving human subjects is initiated until appropriate approvals are documented.
- Ensures that the Group's portfolio of ongoing work/research is monitored to identify potential human safety concerns, deviations from approved protocols, or potential serious or ongoing non-compliance with existing requirements, and should such issues occur, stop the active research program and initiate consultation with HSPO.
- Ensures that stoppages of work/research involving human subjects are reported to the NIST IRB Chair, the HSPO and, if appropriate, the responsible CO or GO.

Principal Investigator

- Facilitates research team compliance with NIST HSPP policies and procedures and completion of required training.
- Completes assigned training and request specific training when necessary.
- Recognizes when proposed and ongoing work/research will potentially involve human subjects as defined by Federal regulations and within this Order, and communicates to Supervisor/Group Leader. If unsure whether work may involve human subjects, PIs are responsible for discussing their proposed research/work with their supervisor.
- Works with Group Leader to prepare: (1) an adequately detailed Human Subjects Research Determination Form to request a determination from the HSPO Director regarding whether a project is a) research, b) research involving human subjects, c) exempt human subjects research, and/or d) non-engagement in research involving human subjects; (2) an adequately detailed Human Research Protocol and all other related required documents; or (3) a request for continuing review.
- Ensures that no research involving human subjects is initiated until appropriate approvals are in place, and that infrastructure and procedures are in place to comply with all requirements associated with the approved work.
- Submits any planned changes to approved work or research, including changes to the research team, through the chain of command (group leader, Division Chief and OU Director) to the HSPO and the NIST IRB, as appropriate, for review, and initiates proposed changes only after appropriate approvals are documented and received.
- Immediately reports any unanticipated potential for human safety concerns, deviations from approved protocols, or potentially serious or ongoing non-compliance with existing requirements to the NIST IRB Chair, the NIST HSPO, Group Leader, Division Chief, OU Director and, if applicable, the responsible Federal Program Officer (FPO) or Contracting Officer's Representative (COR).

- Prepares and submits for approval through the chain of command (Group Leader, Division Chief and OU Director) to the HSPO final reports for human subject research as directed by the NIST IRB.
- Ensures that the research team's portfolio of ongoing work/research is monitored to identify unanticipated potential for human safety concerns, deviations from approved protocols, or potentially serious or ongoing non-compliance with existing requirements, and should such issues occur, is prepared to stop the active research protocol, and stop the research, if directed.
- Ensures potential human subject research is identified in documentation submitted to AMD/GMD if work/research is to be done through a contract or financial assistance award.

Members of Research Team

- Comply with NIST HSPP policies and procedures.
- Complete assigned training and request specific training when necessary.
- Recognize when proposed and ongoing work/research may potentially involve human subjects as defined by Federal regulations and in this Order, and communicate to Supervisor/Group Leader. If unsure whether work involves human subjects, all research team members are responsible for discussing their proposed research/work with their supervisor and the PI.
- Ensure that research involving human subjects is not initiated until appropriate approvals are documented, and comply with all requirements associated with the approved research protocol.
- Report any planned changes to approved work or research team to the PI and initiate proposed changes only after appropriate approvals are documented and received.
- Immediately report any potential human safety concerns, deviations from approved protocols, or potentially serious or ongoing non-compliance with existing requirements to the PI.

Office of the Chief Counsel

- Provides legal support and consultation when requested to any NIST employee, including the HSPO Director and the IRB Chair.
- Reviews associated human subjects documentation as necessary to complete legal sufficiency review of and ensure consistency with all related agreements, including Materials Transfer Agreements, before signature of the agreements by NIST employees.
- Collaborates with the HSPO Director regarding training issues related to legal compliance that may affect research involving human subjects conducted or supported by NIST (e.g., Paperwork Reduction Act, Freedom of Information Act, etc.).

- Monitors proposed regulatory and other legal changes related to Human Subjects research and coordinates with the HSPO Director in the drafting and clearance of NIST comments, as appropriate.
- Serves as an ex officio, non-voting member of the NIST IRB.

Director, Human Subjects Protection Office

- Oversees the implementation of the NIST HSPP day-to-day operations of the NIST HSPO.
- Provides training materials and courses as appropriate for all NIST staff and associates working on NIST research programs potentially involving human subjects.
- Develops the required tools, templates, and procedures required for the implementation of the NIST Order 5501.00.
- Conducts annual quality assurance review of human subjects documentation and makes modifications, as appropriate.
- Determines initial level of review for the proposed Human Subjects Research Protocol based on applicable criteria (*e.g.*, exempt, not engaged in non-exempt research, expedited, or convened IRB review).
- Coordinates with Group Leader, Division Chief (or equivalent), Organizational Unit Director, and NIST IRB Chairperson, as appropriate, including the routing and reviewing of appropriate documents.
- Reviews proposed Human Subjects Research Protocol to make official determinations regarding whether the project is: (1) research, (2) human subjects research; (3) exempt human subjects research; (4) requires review by the IRB, and/or (5) constitutes engagement in non-exempt research.
- Documents that all NIST-supported research involving human subjects that is covered by the Common Rule conducted at or by an external organization has been subject to a review by the NIST HSPO (an institutional review authorized under 15 CFR § 27.112) that verifies the research protocol and all associated documentation (*e.g.*, recruitment material, informed consent forms, etc.) comply with the regulatory requirements and guidance and have been appropriately reviewed and approved. Such work would include research supported by NIST under a contract, grant, cooperative agreement, CRADA, interagency agreement, or other arrangement with NIST.
- Determines whether a project is research, human subjects research, exempt human subjects research, and/or engagement in human subjects research, approves institutional reviews and, as needed, other correspondence to researchers related to review of human subjects research
- Serves as the primary resource for NIST staff on Human Subjects Protection issues.

- Maintains the written policies and procedures to support the institutional FWA requirements.
- Provides administrative oversight to the NIST IRB.
- Provides regular audits and oversight of OU activities that involve research with human subjects.
- Develops, collects, and disseminates metrics for the NIST HSPP, including any time frames required to review and approve human subject research protocols.
- Ensures that all decisions and determinations are communicated to appropriate officials in a timely manner.
- Maintains all records and documentation of NIST conducted or supported Human Subjects activities.
- Provides NIST IRB Chair with a list of research determined to be exempt from NIST IRB review.
- Coordinates with NIST IRB Chair and any external organization that does not have its own cognizant IRB regarding any proposed research involving human subjects.
- When appropriate, facilitate agreements with external IRBs to provide required certifications for research conducted or supported by NIST.
- Participates in the drafting, review and clearance of human subject-related provisions of Federal Funding Opportunities and contracts.
- Monitors proposed regulatory, guidance and policy changes related to Human Subjects research and coordinates with the IRB Chair to arrange for the drafting and clearance of NIST comments, as appropriate.
- Serves as the primary liaison between NIST and OHRP, to include the reporting of all adverse events and incidents of noncompliance.
- With the concurrence of the OU Director, issues stop work order when there are unanticipated risks to subjects or others, and when the work is non-compliant with requirements for human subject protections.
- Completes required training and remains current on federal regulations and guidance related to human subjects protection.

Human Subjects Protections Office Staff

- Work with the Director of the HSPO to implement the NIST P 5500.00 and this directive.
- Provide training on Human Subjects protection to NIST staff.

- Maintain knowledge necessary to interpret current human subjects protection regulations, OHRP guidance, and ethical standards and apply them to research involving human subjects conducted and supported by NIST.
- Serve as a resource to NIST staff in the preparation of documents required for the determination, review, and approval of research that involves human subjects.
- Provide staff support to the NIST IRB.
- Completes required training and remains current on federal regulations and guidance related to human subjects protection.

NIST IRB Chair

- Maintains knowledge necessary to interpret current human subjects regulations, OHRP guidance, and ethical standards and apply them to research involving human subjects at NIST.
- Monitors proposed regulatory, guidance and policy changes related to Human Subjects research and coordinates with the HSPO Director to arrange for the drafting and clearance of NIST comments, as appropriate.
- Presides over meetings of the convened NIST IRB and ensures that the NIST IRB carries out its duly authorized responsibilities as required by federal regulations, ethical principles, applicable state laws, and NIST P 5500.00.
- Reviews and approves submissions that qualify for expedited review pursuant to federal regulations, or delegates such authority to one or more NIST IRB members to conduct such review and approval.
- Notifies the NIST OU Director and researcher in writing of the NIST IRB's approval or disapproval of non-exempt research protocols.
- Ensures that members of the NIST IRB are recruited, appointed and trained such that the NIST IRB is duly qualified to fulfill its obligations.
- Works with the HSPO and the NIST research community to promote communication on the role of the NIST IRB in review of non-exempt research and to work collaboratively with HSPO to provide advice regarding the protection of human subjects.
- Ensures that reports related to safety, noncompliance, unanticipated problems involving risks to human subjects or others, and adverse events, are reviewed, addressed, and reported as required by federal regulations, applicable state laws, and NIST policy.

NIST Institutional Review Board Members

- Complete required training in human subject research protections.

- Review submissions concerning the protection of human subjects in the proposed research and communicates questions, through the HSPO to the PI, concerning the ethical issues related to the protection of human subjects, if any, raised by the research plans.
- Review proposed or continuing research protocol to determine whether it meets criteria for approval or continuation, respectively.

DIRECTIVE OWNER

602 - Human Subjects Protections Office

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	6/15/2014	Jason Boehm	Initial Draft
Ver .01	10/30/2014	Dan Cipra	Formatting updates only
Ver. 02	11/19/2014	Dan Cipra	Incorporated DRB Comments
Ver. 03	7/23/2015	Anne Andrews	Updates to format and HSPO Director responsibilities
Ver, 04	7/30/15	Anne Andrews	Updates to content based on ADLP review

Human Subjects Protection Program

NIST PR 5501.01

Effective Date: 9/3/2015

PURPOSE

This document establishes the procedures for developing and maintaining the Human Subjects Protection Program (HSPP) and Institutional Review Board (IRB) Manual, guides, tools templates, and other similar documents used in review of human subjects research.

APPLICABILITY

This procedure applies to all research conducted or supported by NIST.

REFERENCES

- [15 CFR Part 27](#), the Department of Commerce implementation of the Common Rule for Protection of Human Subjects.
- [45 CFR Part 46](#), Subparts B, C and D, when applicable, Basic Health and Human Services (HHS) Policy for Protection of Human Subjects
- [21 U.S.C. §301](#) et seq., the Federal Food, Drug and Cosmetics Act, as amended.
- [21 CFR Part 56](#), Food and Drug Administration (FDA), Institutional Review Boards
- [21 CFR 312](#), FDA Investigational New Drug Application
- [21 CFR 812](#), FDA Investigation New Device Exemption
- [P 5500.00, Human Subjects Protections](#)
- [O 5501.00, Human Subjects Protection Program](#)
- [The Belmont Report](#): Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, (1978). 44 Fed. Reg. 23192 (Apr. 18, 1979).
- [NIST Institutional Review Board \(IRB\) Charter](#)

PROCEDURES

The Director, Human Subjects Protection Office (HSPO) is responsible for developing the processes and procedures by which all human subjects research conducted or supported by NIST will be reviewed. The following types of documents will be developed and maintained by the

HSPO in support of the HSPP. The minimum timeline for review is noted with each one. The documents will be updated more often if modifications or additions are identified or when there are changes in federal regulations or guidance. Additional Manual chapters, guides, templates and tools will be developed as needed. The documents will be shared with the IRB members, Organizational Unit Directors, human subjects protection staff within the laboratories, and other appropriate groups, committees or offices for review and comment before activation. The Director, HSPO will have final approval and be responsible for activation of the documents. The files will be maintained on the internal website at: <https://inet.nist.gov/hspo>

Manual (reviewed every two years)

- HSPP and IRB Manual

Guides (reviewed every two years)

- Investigator's Guide
- Determinations Guide
- Frequently Asked Questions

Templates and Tools (reviewed annually) may include, but are not limited to the following:

- Research protocol
- Amendment request and checklist
- Continuing review and checklist
- Closure request
- Reportable Events form
- Conflict of Interest form
- Determination Worksheet
- Determination Form and checklist
- Research compliance Principal Investigator (PI) checklist

IRB Tools (reviewed annually) may include, but are not limited to the following:

- IRB review template – new protocol
- IRB review template – amendment
- IRB review template – continuing review
- Research compliance – reviewer worksheet

Education and Training

- Basic Human Subjects Research Awareness
- Ethics in Human Subjects Research
- Good Research Practices
- The NIST HSPP
- Research Determinations

DIRECTIVE OWNER

Human Subjects Protection Office

APPENDICES

- A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	7/15/2015	Anne Andrews (HSPO)	First Draft
Rev. .01	7/15/15	Dan Cipra (M&O)	Formatting Changes and Suggestions
Rev .02	7/30/15	Anne Andrews (HSPO)	Updates based on community expert review
Rev .03	8/28/15	Anne Andrews (HSPO)	Updates based on DRB review

Standard Reference Materials Program

NIST P 5600.00
Effective Date: 7/20/2015

PURPOSE

Industry, government, and academia use the National Institute of Standards and Technology (NIST) reference materials to ensure the highest quality measurements. NIST Standard Reference Materials (SRMs) are key tools for verifying important measurement results, developing new measurement methods, and providing users with tools to assist in establishing traceability of measurement results to NIST.

This directive defines NIST policies for developing, certifying, and distributing NIST SRMs and NIST Reference Materials (RMs). (Note: In this directive, the term SRM refers to both SRM and RM, unless otherwise indicated.)

SCOPE

The policies outlined in this directive apply to all NIST employees involved in the SRM program at NIST laboratory facilities and at joint NIST – third party and third party facilities, and to the entire NIST-level SRM Program, and are not limited to the centralized pre- and post-production support provided by the Office of Reference Materials (ORM).

LEGAL AUTHORITIES AND REFERENCES

- [National Institute of Standards and Technology Act](#) (15 U.S.C. 272(c)(6))
- Cost Recovery
 - 15 U.S.C. [275a](#) and [275c](#)
 - [Office of Management and Budget \(OMB\) Circular A-25](#)
- Earned Net Income and Inventory Replacement Costs
 - [15 U.S.C. 278b\(f\)](#)
- Changes in Policies
 - [15 U.S.C. 278i\(b\)](#)
- Code of Federal Regulations (CFR)
 - [15 CFR 200.104](#)
 - [15 CFR Part 230](#)
- NIST Administrative Manual Subchapter 8.07 [Working Capital Fund](#)
- [NIST SRM Catalogue Special Publication \(SP\) 260](#) and [SRM Price List](#)
- SRM Website <http://www.nist.gov/srm>
- SRM Reporting website <http://msd-i.nist.gov/srmreport/index.jsp>
- SRM Project Tracking System website <http://msd-i.nist.gov/srmtracking/>

POLICY

The NIST Laboratories are responsible for all technical activities including planning, priority setting, and implementation of the development and delivery of NIST Standard Reference Material services, in compliance with the NIST Quality System.

NIST shall recover the full Working Capital Fund (WCF) production costs of each SRM within five years. SRMs must be completed and transferred to finished goods inventory within three years of the initial labor charges on WCF production funds. When the Secretary of Commerce or the Secretary's designee has determined that the interest of the Government would be best served, which may include marketing circumstances, SRMs may be priced at amounts other than those that would recover full production costs.

The Director of the NIST Office of Reference Materials is responsible for ensuring that requirements, processes, and procedures are developed, implemented, and maintained to ensure the highest quality measurements.



Willie E. May
Director



Date

Standard Reference Materials Program

NIST O 5601.00

Effective Date: 7/20/2015

PURPOSE

This purpose of this directive is to define the requirements, roles, and responsibilities for developing, certifying, and distributing NIST Standard Reference Materials (SRMs) and Reference Materials (RMs). It is intended to aid producers of NIST SRMs in the selection and creation of new reference materials and to provide background into the SRM process and the roles of the various NIST organizational units that contribute to the goals of the NIST SRM Program. The objective of the Standard Reference Materials Program is to provide a vehicle for transferring measurement science and technology throughout the scientific community, industry, and commerce. SRMs are key tools for verifying important measurement results, developing new measurement methods, and providing users with tools to assist in establishing traceability of measurement results to NIST. (Note: the term SRM refers to both SRM and RM, unless otherwise indicated.) This directive replaces the NIST Administrative Manual Subchapter 5.19 of the same name.

APPLICABILITY

This directive is applicable to all NIST employees involved in the SRM program at NIST laboratory facilities and at joint NIST – third party and third party facilities, and to the entire NIST-level SRM Program, and are not limited to the centralized pre- and post-production support provided by the Office of Reference Materials (ORM).

REFERENCES

- NIST P 5600.00, Standard Reference Materials
- [15 United States Code \(U.S.C.\)](#) National Institute of Standards and Technology Act
- [15 U.S.C. 275\(a, c\)](#) Authority to charge fees
- [15 U.S.C. 278b\(f\)](#) Earned Net Income and Inventory Replacement Costs
- [15 U.S.C. 278i\(b\)](#) Changes in policies regarding fees for SRMs
- [15 Code of Federal Regulations \(CFR\) 200.104](#) Purpose of the NIST SRM Program
- [15 CFR 230](#) General information and purchase procedures for NIST SRMs
- [The Office of Management and Budget \(OMB\) Circular A-25](#) Establishes federal policy regarding fees

- [NIST SRM Catalogue Special Publication \(SP\) 260](#) and [SRM Price List](#)
- [SRM Website](#)
- [SRM Reporting Site](#)
- [SRM Project Tracking System](#)

DEFINITIONS

Certified Reference Material (CRM) – reference material (RM) characterized by a metrologically valid procedure for one or more specified properties, accompanied by an RM certificate that provides the value of the specified property, its associated uncertainty, and a statement of metrological traceability. (ISO Guide 30: 2015)

Costs on the Books/Work-in-Process – the amount of NIST Working Capital funds invested in an SRM for which transfers to stock and production costs remain.

NIST Certificate of Traceability – Document stating the purpose, protocols, and measurement pathways that support claims by an NIST Traceable Reference Material (NTRM) to specific NIST standards or stated references. No NIST certified values are provided, but rather the document references a specific NIST report of analysis, bears the logo of the U.S. Department of Commerce, the name of NIST as a certifying body, and the name and title of the NIST officer authorized to accept responsibility for its contents.

NIST Certified Value – A value reported on an SRM certificate or certificate of analysis for which NIST has the highest confidence in its accuracy in that all known or suspected sources of bias have been fully investigated or accounted for by NIST. (NIST SP 260-136)

NIST Information Value – a value that is considered to be of interest and use to the SRM user, but insufficient information is available to assess adequately the uncertainty associated with the value or only a limited number of analyses were performed. Information values cannot be used to establish metrological traceability.

NIST Reference Material – Material issued by NIST with a report of investigation instead of a certificate to: (1) further scientific or technical research; (2) determine the efficacy of a prototype reference material; (3) provide a homogeneous and stable material so that investigators in different laboratories can be ensured that they are investigating the same material; and (4) ensure availability when a material produced and certified by an organization other than NIST is defined to be in the public interest or when an alternate means of national distribution does not exist. A NIST RM meets the ISO definition for a RM and may meet the ISO definition for a CRM, depending on the statements of traceability contained in its Report of Investigation.

NIST Reference Value – noncertified values that represent the best estimate of the true values based on available data; however, the values do not meet the NIST criteria for certification and are provided with associated uncertainties that may reflect only

measurement reproducibility, may not include all sources of uncertainty, or may reflect a lack of sufficient statistical agreement among multiple analytical methods. (NIST SP 260-136)

NIST RM Report of Investigation – Document issued with a NIST RM that contains all the technical information necessary for proper use of the material, the logo of the U.S. Department of Commerce, and the name and title of the NIST officer authorized to issue it. Reports of Investigation may contain reference values, information values or statements related to the homogeneity and stability of studied parameters, but they do not contain certified values.

NIST Report of Analysis (ROA) – Document containing the certification of the material and including such information as the base material used, how the SRM was manufactured, the certification method(s) and description of procedures, outside collaborators, instructions for use, special instructions for packaging, handling, and storage, and plan for stability testing. The ROA is intended for internal NIST use only.

NIST Standard Reference Material® (SRM®) – A CRM issued by NIST that also meets additional NIST-specific certification criteria and is issued with a certificate or certificate of analysis that reports the results of its characterizations and provides information regarding the appropriate use(s) of the material (NIST SP 260-136). Note: An SRM is prepared and used for three main purposes: (1) to help develop accurate methods of analysis; (2) to calibrate measurement systems used to facilitate exchange of goods, institute quality control, determine performance characteristics, or measure a property at the state-of-the-art limit; and (3) to ensure the long-term adequacy and integrity of measurement quality assurance programs. The terms “Standard Reference Material” and “SRM,” and the diamond-shaped logo which contains the term “SRM,” are registered with the United States Patent and Trademark Office.

NIST SRM® Certificate or Certificate of Analysis – In accordance with latest published version of ISO Guides 30 and 31, a NIST SRM certificate is a Reference Material Certificate containing the name, description, and intended purpose of the material, the logo of the U.S. Department of Commerce, the name of NIST as the certifying body, instructions for proper use and storage of the material, certified property value(s) with associated uncertainty(ies), method(s) used to obtain property values, the period of validity, if appropriate, and any other technical information deemed necessary for its proper use. A Certificate is issued for an SRM certified for one or more specific *physical or engineering performance* properties and may contain NIST reference, information, or both values in addition to certified values. A Certificate of Analysis is issued for an SRM certified for one or more specific *chemical* properties. Note: ISO Guide 31 is updated periodically; check with ISO for the latest version.

NIST Traceable Reference Material (NTRM^{CM}) – A commercially-produced reference material with a well-defined traceability linkage to existing NIST standards for chemical

measurements. This traceability linkage is established via criteria and protocols defined by NIST to meet the needs of the metrological community to be served (NIST SP 260-136). Reference materials producers adhering to these requirements are allowed use of the NTRM trademark. A NIST NTRM may be recognized by a regulatory authority as being equivalent to a CRM.

Reference Material (RM) – material, sufficiently homogeneous and stable with respect to one or more specified properties, which has been established to be fit for its intended use in a measurement process. (ISO Guide 30: 2015)

Reference Material Certificate – document containing the essential information for the use of a CRM, confirming that the necessary procedures have been carried out to ensure the validity and metrological traceability of the stated property values (ISO Guide 30: 2015)

REQUIREMENTS

- NIST shall develop, certify, and distribute SRMs available for use in areas such as industrial materials production and analysis, environmental analysis, health measurements, and basic measurements in science and metrology to ensure accurate and compatible measurements world-wide.
- NIST shall provide SRMs when:
 - a. A measurement problem has been identified for which a Certified Reference Material from NIST has been determined to be the most effective means for providing the required measurement accuracy, traceability, or both;
 - b. Industry-wide reference materials or standards for commerce are not otherwise available, or are needed from a neutral supplier; and/or
 - c. Continuing availability of a highly characterized material from a common source is important to science or industry.
- NIST Laboratories shall set all priorities and make all technical decisions related to their SRM research, development and production activities.
- The NIST Budget Division shall determine, on a NIST Laboratory by NIST Laboratory basis, the *annual* estimate of the development and production funds available for investment in SRMs.
- SRMs must be completed and transferred to finished goods inventory within three years of the initial labor charges on Working Capital Fund (WCF) production funds.
- In order for the SRM production to be considered complete, the NIST Laboratory's technical staff shall submit (1) draft certificate, (2) report(s) of analysis, (3) project completion memorandum and (4) units of the material.
- The full WCF production costs of an SRM shall be recovered within five years. Full cost recovery pricing is to be based on (i) the full production costs, (ii) the estimated number-

of-years supply the units represent, and (iii) the basis for the estimate provided by the NIST Laboratory technical staff.

- The Laboratory's technical staff shall work with the ORM to complete post-production activities including: documentation review, pricing, web updates, sales, marketing, packaging, storage, distribution, reporting, and policy management.
- ORM may assist with candidate material processing, blending and packaging as requested by a NIST Laboratory.
- If a NIST Laboratory fails to deliver an SRM and no payback waiver has been received from the Associate Director of Measurement Services (ADMS), the NIST Laboratory shall repay the amount of WCF invested in the SRM with its Scientific and Technical Research and Services (STRS) funds.

SRM RESOURCES

The following describes the types of funding and resources available to support NIST SRM activities and the appropriate use of each.

a. STRS appropriated funds can support the *research, development and production* phases of an SRM. During the *research* phase, new measurement concepts and methods are explored.

(1) A NIST Laboratory's SRM research activities are funded with its own STRS allocation according to each NIST Laboratory's strategic priorities.

(2) NIST's STRS budget initiative requests can include transfers to the Working Capital Fund for the production of SRMs. However, the amount of NIST STRS that can be transferred to the WCF is limited by the authority specified in appropriations legislation.

(3) If the Congress grants transfer authority not specifically tied to or needed by a budget initiative, the NIST Budget Division will solicit interest from each NIST Laboratory in transferring their own STRS to the WCF for SRM production. The NIST Budget Division will then distribute the total annual transfer amount equally among the interested NIST Laboratories.

b. Service Development (SD) funds support the *development* of a prototype of future SRMs and are used to resolve any material or technical issues prior to investing WCF Production funds.

(1) SD provides a means of funding projects to demonstrate the feasibility of a new SRM base material or certification protocol and to establish the final procedures for manufacturing the SRM before production activities are funded on the NIST Working Capital Fund.

(2) The amount of SD funds available in any given year is determined for each NIST Laboratory by the NIST Budget Division based on each NIST Laboratory's anticipated SD collections through the sale of its SRMs.

- c. WCF resources may only be used to finance the *production* of a saleable SRM product.
- (1) WCF resources are only used when *all* material and technical issues have been resolved in the research and development phases.
 - (2) The amount of WCF production funds available in any given year is determined for each NIST Laboratory by the NIST Budget Division based on previous and projected rates of WCF replenishment through the sale of the NIST Laboratory's SRMs. This sales estimate is adjusted for each NIST Laboratory's prior year carryover to determine the NIST Laboratory's total annual WCF production allocation.
- d. Federal government agency funds or services may be provided to NIST for the research, development, or production, or all three phases, of an SRM, as specified in the agreement between NIST and the other federal government agency.
- (1) Procedures for work sponsored by outside organizations, both federal and non-federal, are contained in [Administrative Manual Subchapter 8.05 "NIST Work Performed for Others"](#). The Counsel for NIST must be consulted if circumstances arise that are not covered in this order or [Administrative Manual Subchapter 8.05 "NIST Work Performed for Others"](#).
- e. Non-federal government (NFG) sponsor funds or services for SRM work may be provided only after the appropriate approvals have been received by the NIST Laboratory.
- (1) Agreements with NFG sponsors involving SRMs must be reviewed and approved by the NIST Budget Division and the Counsel for NIST prior to work performed.
- f. Donated material or services may be accepted to develop or produce an SRM, but these donations must adhere to the guidelines in [Administrative Manual Subchapter 8.10, Gifts and Requests](#).
- g. Stability testing funds support the cost of testing units already in inventory for which deterioration is expected to occur.
- h. Operations funding supports the Office of Reference Materials administrative support and centralized business and information services expenses related to SRMs.

RESPONSIBILITIES

NIST Laboratory

- Plans, sets priorities, funds, and implements the development, production, delivery, and quality of SRMs;
- Establishes technical criteria for the development and certification of SRMs;
- Determines specifications for and acquires material;

- Provides ORM with specifications for material preparation, if appropriate, and storage of units;
- Ensures that all NIST WCF resources assigned to it are used appropriately and properly accounted for;
- Determines the number of units to be produced and the appropriate time period for cost recovery with a maximum of five years to calculate the unit sales prices, as well as provides the basis for the annual unit sales estimate;
- Develops and carries out a material stability monitoring plan and perpetuation plan for each new SRM;
- Performs continuous assessment of customer needs and requirements for SRMs;
- Prepares and packages material, or requests ORM to do so;
- Provides customer technical support as needed;
- Establishes and maintains a quality system that assures quality in the results of its measurement services; and
- Provides representation on relevant national and international committees for the technical aspects of SRMs.

Office of Reference Materials (ORM)

- Provides guidance to the NIST Laboratories, upon request, for the development, production, and certification of SRMs;
- Evaluates the business case of projects that have been submitted by the NIST Laboratories for WCF and SD funding and communicates the results of that evaluation to the NIST Budget Division;
- Performs activities related to preparing, packaging, labeling, pricing, marketing, warehousing, selling, and distributing SRMs;
- Reviews certificates for NIST-wide uniformity and ISO Guide compliance and prepares and maintains other documentation (i.e. safety data sheets) related to SRMs;
- Prepares and updates the Special Publication (SP) 260 SRM catalog and price list;
- Prepares and issues other documents such as journal articles, brochures, and newsletters that provide current information about SRMs;
- Exhibits SRMs and related publications and documentation at technical meetings, conferences, and trade shows;
- Provides the necessary information, reports, and administrative support to NIST customers and NIST Laboratories; and

- Provides national and international representation for business and policy aspects of SRMs.

Statistical Engineering Division (SED)

- Assists in the design of sampling and measurement strategies for certification of SRMs;
- Provides technical guidance on the implementation of NIST uncertainty policy;
- Develops standardized statistical design and analysis templates that can be used by NIST Laboratory personnel to carry out statistical analyses for classes of SRMs that follow fixed approaches;
- Provides training on the proper use, interpretation, and limitations of these templates;
- Provides data analysis and uncertainty assessment for SRMs for which appropriate standardized analysis templates are not available; and
- Certifies the computation for unit values and stated uncertainties, as appropriate.

Office of Financial Resource Management - Budget Division

- Reviews and approves the annual SRM Operations budget as proposed by ORM;
- Reviews and sets annual SRM surcharge levels;
- Determines the annual Service Development (SD) and WCF Production funding levels, including carryover, and communicates to ORM the allocation levels by NIST Laboratory;
- Reviews and approves WCF Stock Transfer Notices (STNs) that transfer units to stock and establish unit sales prices;
- Reviews and approves the annual inflationary factor for materials and labor as proposed by ORM for calculation of the replacement surcharge; and
- Monitors expense and income, work-in-process, and sales activities for the SRM Program.

Office of Financial Resource Management – Finance Division

- Handles all NIST collections for SRMs sold;
- Handles the deferral of Service Development income in excess of expenses at year-end; and
- Serves as liaison for all financial audit activities regarding the SRM Program.

DIRECTIVE OWNER

640.00 – Office of Reference Materials (ORM)

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	11/20/12	Dan Cipra	Initial Draft
Rev 1	1/7/2015	Dan Cipra	Formatting changes, sent back to DO for internal vetting
Rev 2	1/13/2015	Robert Watters	Accepted formatting changes
Rev. 3	6/8/2015	Nancy Parrish	DRB Comments incorporated

Managing Public Access to Results of Federally Funded Research Policy

NIST P 5700.00

Effective Date: 6/26/2015

I. PURPOSE

Pursuant to the Office of Science and Technology Policy (OSTP) Memorandum for the Heads of Executive Departments and Agencies of February 22, 2013, *Increasing Access to the Results of Federally Funded Scientific Research*¹, Executive Order of May 9, 2013, *Making Open and Machine Readable the New Default for Government Information*², and the Office of Management and Budget (OMB) Memorandum for the Heads of Executive Departments and Agencies of May 9, 2013, *Open Data Policy – Managing Information as an Asset*³, this directive establishes a governing policy for managing data and providing public access to results of federally funded research, i.e., scientific research results, including data and NIST's scholarly and technical publications, in all media.

II. SCOPE

This policy applies to⁴:

1. Research data⁵ means the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or communications with colleagues. This "recorded" material excludes physical objects (e.g., laboratory samples).

Research data also does not include:

¹ http://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf

² <http://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government>

³ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>

⁴ This policy applies to all NIST employees, including full- and part-time employees, temporary government employees, and special government employees, and to associates engaged in research activities at or for NIST, to the extent allowed by law and the terms of the Associate's agreement. A non-NIST organization that publishes scholarly and technical material, including data, through activities funded wholly or in part by NIST through a grant, cooperative agreement, contract, or other agreement, must manage public access to published scholarly and technical material, including data, as specified by NIST in the terms and conditions of the grant, cooperative agreement, contract, or other agreement between NIST and the non-NIST organization.

⁵ For purposes of this policy, NIST is adopting the definition of "research data" provided in 2 C.F.R. §200.315 (e)(3). <http://www.gpo.gov/fdsys/pkg/CFR-2014-title2-vol1/pdf/CFR-2014-title2-vol1-sec200-315.pdf>

Trade secrets, commercial information, materials necessary to be held confidential by a researcher until they are published, or similar information which is protected under law; and

personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study.⁶

2. Published scholarly and technical material, which may include data.

III. LEGAL AUTHORITIES AND REFERENCES

1. Legal Authority. [Executive Office of the President, Executive Order, Making Open and Machine Readable the New Default for Government Information, 9 May 2013.](#)
2. References
 - a. [5 U.S.C. § 552, Freedom of Information Act](#)
 - b. [15 U.S.C. 271 et seq., National Institute of Standards and Technology Act](#)
 - c. [17 U.S.C. 105, Subject matter of copyright: United States Government works](#)
 - d. [15 U.S.C. §§ 290-290f, Standard Reference Data Act](#)
 - e. [44 U.S.C. § 3501 et seq., Paperwork Reduction Act of 1995](#)
 - f. [Public Law 107-347, E-Government Act of 2002, § 207.](#)
 - g. [Public Law 111-358, America COMPETES Reauthorization Act of 2010, § 103.](#)
 - h. [5 CFR Part 1320, Controlling Paperwork Burdens on the Public](#)
 - i. [15 CFR Part 4, Subpart A, Freedom of Information Act](#)
 - j. [Executive Office of the President, OMB, Memorandum for the Heads of Executive Departments and Agencies \(MHEDA\), Open Data Policy – Managing Information as an Asset, M-13-13, 9 May 2013.](#)
 - k. [Executive Office of the President, OSTP, MHEDA, Increasing Access to the Results of Federally Funded Scientific Research, 22 February 2013.](#)
 - l. [Executive Office of the President, OMB, MHEDA, Open Government Directive, M-10-06, 8 December 2009.](#)
 - m. [Executive Office of the President, MHEDA, Transparency and Open Government, 74 FR 4685, 21 January 2009.](#)

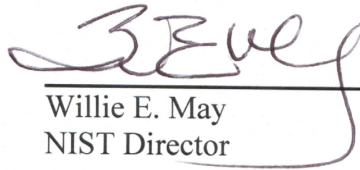
⁶ To the extent this information is used in research, for example, electronic health records, the policy applies, but such information may only be made publicly available consistent with applicable laws, regulations and policies. NIST employees must consult with the NIST Human Subjects Protections Office and the Office of the Chief Counsel for NIST before making such information public.

- n. [OMB, Circular A-130, Management of Federal Information Resources, 28 November 2000.](#)

IV. POLICY

To the extent feasible and consistent with law, agency mission, resource constraints, and U.S. national, homeland, and economic security, NIST will promote the deposit of scientific data arising from unclassified research and programs, funded wholly or in part by NIST, except for Standard Reference Data,⁷ free of charge in publicly accessible databases. Subject to the same conditions and constraints listed above, NIST also intends to make freely available to the public, in publicly accessible repositories, all peer-reviewed scholarly publications arising from unclassified research and programs funded wholly or in part by NIST.

The NIST Associate Director for Laboratory Programs is responsible for ensuring that requirements, processes, and procedures are developed, implemented, and maintained to ensure that NIST makes this information available to the public. The NIST Associate Director for Laboratory Programs may delegate this authority.


Willie E. May
NIST Director

6/26/15
Date

⁷ NIST has explicit authority to license Standard Reference Data. See [15 U.S.C. §§ 290-290f, Standard Reference Data Act](#)

Managing Public Access to Results of Federally Funded Research

NIST O 5701.00
Effective Date: 6/26/2015

I. PURPOSE

This order describes requirements and responsibilities for managing public access to results of scientific research funded wholly or in part by NIST.

II. APPLICABILITY

This order applies to:¹

1. All NIST employees, including full- and part-time employees, temporary government employees, and special government employees, who record factual material commonly accepted in the scientific community as necessary to validate research findings as part of their employment.
2. All NIST employees, including full- and part-time employees, temporary government employees, and special government employees, who publish scholarly and technical material, including data, as part of their employment.
3. All NIST associates engaged in research activities at or for NIST who record factual material commonly accepted in the scientific community as necessary to validate research findings, to the extent allowed by law and the terms of the associate's agreement.
4. All NIST associates engaged in research activities at or for NIST who publish scholarly and technical material, that may include data, to the extent allowed by law and the terms of the associate's agreement,
5. All NIST employees involved in the awarding and/or oversight of NIST contracts, financial assistance awards, or other agreements.
6. All NIST employees involved in the drafting, negotiation, implementation and oversight of agreements under which NIST employees perform research for other parties.

III. REFERENCE

- NIST P 5700.00 NIST Policy on Managing Public Access to Results of Federally Funded Research

¹ A non-NIST organization that publishes scholarly and technical material, including data, through activities funded wholly or in part by NIST through a grant, cooperative agreement, contract, or other agreement, must manage public access to published scholarly and technical material, including data, as agreed to by NIST and that organization in the terms and conditions of the grant, cooperative agreement, contract, or other agreement between NIST and the non-NIST organization.

IV. DEFINITIONS²

Accepted Manuscript:³ The version of a journal article that has been accepted for publication in a journal.

Data: Research data means the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or communications with colleagues. This “recorded” material excludes physical objects (e.g., laboratory samples). Research data also does not include:

- (i) Trade secrets, commercial information, materials necessary to be held confidential by a researcher until they are published, or similar information which is protected under law; and
- (ii) Personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study.⁴

For purposes of this order, NIST considers the contents of laboratory notebooks to be preliminary analyses.

Data Management Plan (DMP): A defined plan for the management of data that provides, at a minimum, a summary of activities for data generation, a summary of the types of data generated by the relevant activities, the plans for preservation of the generated data, and a description of the appropriate level of access for the generated data.

Digital Object Identifier (DOI): A string of characters used to identify an object such as an electronic document. A group of digital objects may be associated with a Persistent Identifier (*see* Persistent Identifier definition below).

Discoverability: the ability of a piece of content or information to be found.

Federal Digital System (FDSys): A system within the U.S. Government Printing Office (GPO) that will serve as NIST’s repository for NIST Technical Series publications as well as other papers that have not been reviewed through an external publisher’s peer-review process (e.g., conference proceedings, reports); <http://www.gpo.gov/fdsys/>.

Final Published Article: The version of record⁴; the publisher’s authoritative copy of the final manuscript, including all modifications resulting from the journal’s review process, copyediting, stylistic edits, and formatting.

Metadata: Standardized descriptive values that explain, locate, or enable the retrieval of data or publications. (*See*, for example, <https://project-open-data.cio.gov/v1.1/schema/>.) This does not include ‘domain metadata’ which provides the user with common understanding of

² All definitions are in the context of this directive and are listed in alphabetical order. In cases where a definition is adopted from a reference, the reference is cited in a footnote.

³ [National Information Standards Organization, *Journal Article Versions \(JAV\): Recommendations of the NISO/ALPSP JAV Technical Working Group*, 2008.](#)

⁴ [2 C.F.R. §200.315 \(e\)\(3\)](#)

the meaning or semantics of the data, to ensure correct and proper use and interpretation of the data by its owners and users.

NIST Editorial Review Board (ERB): The NIST ERB is a Standing Administrative Committee as defined in NIST O 1005.00, NIST Administrative Committees, and currently comprises separate Editorial Review Boards located at Boulder (BERB), JILA (JERB), and Gaithersburg (WERB).

NIST Editorial Review System (ERS): The NIST ERS is the program through which manuscripts are reviewed and approved prior to submission by the author to a publisher.

NIST Enterprise Data Inventory (EDI): A searchable system containing a comprehensive listing of NIST datasets with associated metadata, including an indication of whether they may be made publicly available (i.e., release is permitted by law, regulation and policy, subject to all privacy, confidentiality, security, and other valid requirements) and whether they are currently available to the public.

NIST Public Access Archive System: See definitions of PubMed Central and Federal Digital System.

NIST Scholarly and Technical Publications: Publications, including final published articles and the NIST Technical Series publications, which describe the results of NIST technical activities.

NIST Technical Series Publications: NIST scholarly and technical publications published by or for NIST; http://www.nist.gov/nvl/nist_series_publications.cfm.

Open Access: Unrestricted online access to a scholarly or technical publication.

Persistent Identifier: A unique label for a data resource.

PubMed Central (PMC): PubMed Central, maintained by the National Institutes of Health. Beginning October 1, 2015, this platform will serve as NIST's repository for peer-reviewed publications; <http://www.ncbi.nlm.nih.gov/pmc/>.

V. REQUIREMENTS

1. Data

- a. **Data Management Plans (DMPs)**. The requirements stated below are the minimum requirements for DMPs. A NIST Organizational Unit (OU) or Office may expand these requirements to meet the needs of activities within that OU or Office or across OUs or Offices.

NIST OU Directors and Office Directors are responsible for ensuring that DMPs are developed and maintained for all data generated in their respective OU or Office.

Responsibility for the development and maintenance of the DMPs may be delegated as determined by the OU Director or Office Director.

In cases where multiple OUs or Offices share a common data-generating activity, the Director of the OU or Office with the greatest role in directing the activity, i.e., the

champion, will determine whether to develop one DMP or multiple DMPs specific to that activity in a manner determined by the champion.

An OU Director or Office Director must ensure that development and maintenance of DMPs is included in performance plans for NIST employees within their OU or Office who have those responsibilities.

All research data generated that results from activities funded wholly or in part by NIST must be covered by a relevant DMP. These plans must contain, at a minimum, the following elements:

- (1) **Summary of activities:** a summary of activities that generate data.
- (2) **Data types and classification:** a summary of the data types generated by the identified activities. *Data should be categorized, at a minimum, according to the data categories presented in the NIST Data Taxonomy and Actions/Consequences for Data Categories, provided in Appendix A of this Order, as applicable.*
- (3) **Preservation:** a plan for storage and maintenance of the data generated by the identified activities, in both the short-term and long-term (if relevant). *Data should be preserved, at a minimum, according to the preservation consequence levels defined in the NIST Data Taxonomy and Actions/Consequences for Data Categories, provided in Appendix A of this Order, as applicable, and in accordance with applicable records retention requirements.*
- (4) **Review, Discoverability, and Access:** a plan describing whether and how the data generated by the identified activities will be reviewed and made available to the public and how the metadata describing it will be entered into the NIST Enterprise Data Inventory (EDI). The plan should describe any known access restrictions for the data and/or metadata, if appropriate. *Data should be made discoverable, at a minimum, according to the discoverability consequence levels defined in the NIST Data Taxonomy and Actions/Consequences for Data Categories, provided in Appendix A, as applicable.*

b. NIST Enterprise Data Inventory (EDI). All metadata for NIST data, as applicable, must be entered into the NIST EDI based on the discovery consequence levels (*see* Appendix A, Section III.3. of this Order) and OU or Office guidance.

- 2. NIST Scholarly and Technical Publications.** All NIST scholarly and technical publications with a publication date of October 1, 2015 or later must be submitted to the NIST public access archive system (*see* Section IV. Definitions) no later than 12 months following publication.

VI. RESPONSIBILITIES

1. NIST Director

- (1) Controls and manages NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research.
- (2) Ensures coordination of the management of public access to results of federally funded research with non-NIST organizations, as applicable.

2. Associate Director for Laboratory Programs (ADLP)

- (1) Implements and provides oversight for maintenance of, and compliance with, NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research.
- (2) Ensures the availability of appropriate resources for managing public access to results of federally funded research.
- (3) Reviews, approves, and evaluates the effectiveness of NIST OU and Office plans for managing public access to results of federally funded research
- (4) Coordinates collaboration and cooperation on implementation of the NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research across NIST and with the Department of Commerce and other federal agencies.
- (5) With the Associate Director for Management Resources (ADMR) and the Associate Director for Innovation and Industry Services (ADIIS), coordinates with relevant OUs and Offices in their infrastructure planning and implementation to promote interoperability across NIST.
- (6) Oversees the activities of the Directors of the Operating Units within the ADLP Directorate in supporting NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research, as applicable.

3. Associate Director for Management Resources

- (1) Facilitates the provision of NIST-level infrastructure to manage public access to results of federally funded research.
- (2) Ensures the development and deployment of training, awareness, and outreach activities pertaining to the management of public access to results of federally funded research.
- (3) With the ADLP and ADIIS, coordinates with relevant OUs and Offices in their infrastructure planning and implementation to promote interoperability across NIST.
- (4) Oversees the activities of the Chief Information Officer and the Directors of the Information Services Office and Office of Acquisition and Agreements Management in supporting NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research, as applicable.

4. Associate Director for Innovation and Industry Services

- (1) Oversees the activities of the Directors of the Advanced Manufacturing National Program Office, the Baldrige Performance Excellence Program, the Economic Analysis Office, the Hollings Manufacturing Extension Partnership Program, the Technology Innovation Program, and the Technology Partnerships Office in supporting NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research, as applicable.

5. Chief Information Officer (CIO)

- (1) Manages NIST-level information technology infrastructure to support NIST's provision of public access to results of federally funded research.
- (2) Ensures that the NIST EDI is available to NIST employees and that NIST inventory records are provided to the Department of Commerce and government-wide inventories in the necessary format, per Office of Management and Budget requirements.
- (3) Supports NIST OU Directors' and Office Directors' responsibilities (*see* Section VI.8. of this Order), as applicable.

6. Director, Information Services Office

- (1) Works with the Office of Information Systems Management (OISM) to ensure implementation and operation of the NIST EDI.
- (2) Manages creation and maintenance of persistent identifiers for NIST Technical Series Publications.
- (3) Provides consultation and educational materials for NIST employees on:
 - a. managing data and providing public access to results of federally-funded research, including use of the NIST EDI, and
 - b. the NIST review process, as applicable, for results of federally funded research that are intended for dissemination in any media in accordance with Administrative Manual Subchapter 4.09, NIST Technical Communications Program.
- (4) Facilitates search and access to metadata for NIST data or final published articles or NIST Technical Series Publications for the public.
- (5) Supports NIST OU Directors' and Office Directors' responsibilities (*see* Section VI.8. of this Order), as applicable.

7. Director, Office of Acquisition and Agreements Management (OAAM)

- (1) Works with the Directors of NIST OUs and Offices to ensure that, beginning October 1, 2015, grants, cooperative agreements, contracts, and other agreements through which NIST funds activities, wholly or in part, include requirements for managing data and publications, as specified in the terms and conditions of the grant, cooperative agreement, contract, or other agreement with the non-NIST organization,

consistently with the NIST Policy and Order for Managing Public Access to Results of Federally Funded Research.

8. OU Director or Office Director

- (1) Implements ADLP-approved plan to manage public access to results of activities funded wholly or in part by NIST within his/her OU or Office.
- (2) Works with other offices, e.g., OISM and the Information Services Office, to manage public access to results of activities funded wholly or in part by NIST.
- (3) Reviews data to ensure that no personally or business identifiable information is present and that appropriate protective measures are in place prior to making it publicly available; authority to carry out this responsibility may be delegated to the Division Chief or equivalent, per Administrative Manual Subchapter 4.09, NIST Technical Communications Program.
- (4) Ensures that his/her OU or Office prioritizes the discoverability (based on the discovery consequence levels in Appendix A, Section III.3. of this Order) and publication of applicable OU or Office datasets based on stakeholder needs and resources required.

9. Supervisory Employee within an OU or Office within the ADLP Directorate

- (1) Ensures activities under his/her direction are in compliance with his/her OU or Office plans to manage public access to results of federally funded research.
- (2) Ensures employees under his/her supervision meet employee-level requirements of his/her OU or Office plans to manage public access to results of federally funded research.
- (3) Works with OAAM to ensure that, beginning October 1, 2015, grants, cooperative agreements, contracts, and other agreements through which NIST funds activities, wholly or in part, include requirements for managing data and publications, as specified in the terms and conditions of the grant, cooperative agreement, contract, or other agreement with the non-NIST organization, consistently with the NIST Policy and Order for Managing Public Access to Results of Federally Funded Research.

10. Non-Supervisory Employee within ADLP Directorate

- (1) Complies with the employee-level requirements of his/her OU or Office plans to manage public access to results of federally funded research: prepares and executes DMPs as specified by the OU or Office plans to manage public access to results of federally funded research, and as applicable,
 - a. provides metadata for NIST data to the NIST EDI or other publicly available repositories, as applicable,
 - b. if data are tagged as available to the public in the EDI, provides data in open formats via publicly available repositories or upon request and to the extent feasible, directly to the requestor, free of charge unless otherwise excepted, and

- c. provides publications dated October 1, 2015 and later to the NIST public access archive system no later than 12 months following publication.
- (2) Works with OAAM to ensure that, beginning October 1, 2015, grants, cooperative agreements, contracts, and other agreements through which NIST funds activities, wholly or in part, include requirements for managing data and publications, as specified in the terms and conditions of the grant, cooperative agreement, contract, or other agreement with the non-NIST organization, include requirements for managing data and publications consistently with the NIST Policy and Order for Managing Public Access to Results of Federally Funded Research.

VII. DIRECTIVE OWNER

600 – Associate Director for Laboratory Programs

VIII. APPENDICES

- A. NIST Data Taxonomy and Actions/Consequences for Data Categories
- B. Revision History

APPENDIX A

NIST DATA TAXONOMY AND ACTIONS/CONSEQUENCES FOR DATA CATEGORIES

I. PURPOSE

The purpose of this taxonomy is to define a collection of terms and concepts that describe classes and categories scientific data arising from unclassified research and programs funded wholly or in part by NIST⁵, as well as policy requirements, actions, and consequences that might apply to those categories as a result of requirements expressed in the Office of Science and Technology Policy (OSTP) Open Data Memorandum, OMB Memorandum M-13-13, and Executive Order 13642. (*See* NIST Policy P 105.01.) In the context of these requirements, research data is defined as “the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or communications with colleagues.”⁶

Although the categories in the NIST data taxonomy are arranged in a pyramid, they are not strictly hierarchical. Categories range from working data to standard reference data (SRD) (*see* Figure 1). The goal of this document is to achieve a shared understanding of the data management space at NIST, not to make policy choices or to define requirements or recommend procedures. This vocabulary is intended to enable discussions among NIST management and technical staff to support NIST’s data management Policy and Order.

⁵ A non-NIST organization that publishes scholarly and technical material, including data, through activities funded wholly or in part by NIST through a grant, cooperative agreement, contract, or other agreement, must manage public access to published scholarly and technical material, including data, as agreed to by NIST and that organization in the terms and conditions of the grant, cooperative agreement, contract, or other agreement between NIST and the non-NIST organization.

⁶ For purposes of this policy, NIST is adopting the definition of “research data” provided in 2 C.F.R. §200.315 (e)(3). <http://www.gpo.gov/fdsys/pkg/CFR-2014-title2-vol1/pdf/CFR-2014-title2-vol1-sec200-315.pdf>

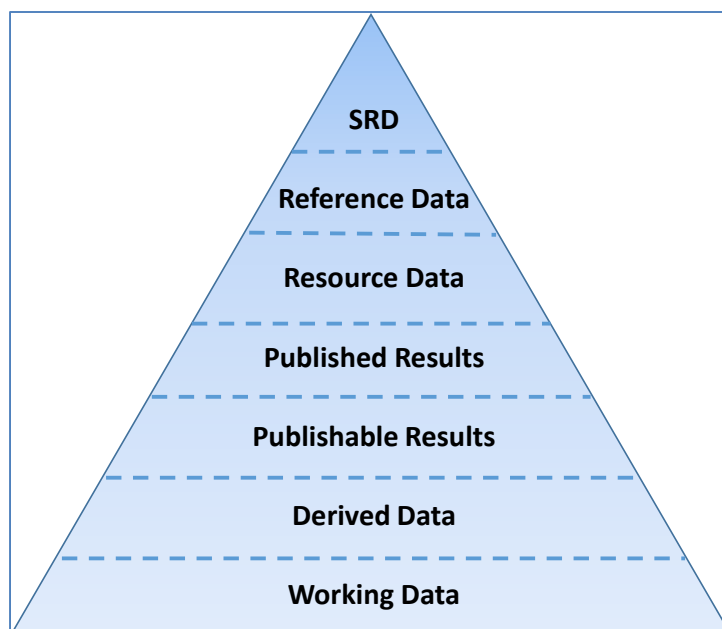


Figure 1. Data pyramid describing the categories of NIST data, ranging from “Working Data” to “Standard Reference Data (SRD)”

II. DATA CATEGORIES

The main categories envisioned for NIST data have been arranged in the form of a “data pyramid,” (Figure 1) recognizing that in general the volume of data decreases as you move from the bottom of the pyramid toward the top. This is an oversimplification, and several competing dimensions for characterizing and distinguishing data classes have been combined into this one view for reasons of simplicity and compactness. However, this simplified diagram (Figure 1) provides a useful breakdown of data classes for the narrow context of discussing data management plans and NIST data curation and dissemination policies.

Several classes of data are described in the pyramid, with the following definitions:

1. Working Data

The digital equivalent of entering data in a laboratory notebook. Working data may be raw observational data that is acquired directly from an instrument or a measurement system, or digital values acquired or generated during experiments or simulations. In some cases the researcher responsible for generating the working data may determine that this data has immediate value and is worth preserving, or the researcher may expect that the data will have

value after it has been manipulated or further evaluated, and the data has the potential to develop into a publication or will be used to draw conclusions. In other cases working data may be recognized as not appropriate for broader use in its present form. It may have value to the data producers and their collaborators, but it should be recognized that the data could be easily misinterpreted by people not closely involved in its production because some metadata and important facts about its status or acquisition are not readily available beyond the immediate research team (e.g., adequate metadata for re-purposing is not attached to the data itself, or expending resources to codify needed metadata is not justified, etc.).

2. Derived Data

Underpins the conclusions provided in a publication or report. Derived data comes from working data that has been manipulated, analyzed, processed, or evaluated in some way. The data must have passed some minimal (perhaps *ad hoc*) evaluation and be considered by the responsible researcher (typically the data producer) to be ready for the next steps in the workflow or project/product development effort.

3. Publishable Results

All final or summary results that comply with relevant NIST policies (e.g., SI units, uncertainty statements), that have been reviewed internally and approved by an appropriate NIST authority, and that could be published either in a scientific publication or as a standalone data product.

4. Published Results

Results that are publishable and that are contained in a document that has been reviewed and approved for publication by the necessary NIST organizational authorities, submitted to its intended publisher, and made public.

5. Resource Data

Data used to underpin, support, or defend decisions, actions, or positions of NIST.

6. Reference Data (RD)⁷

Data similar in many characteristics to SRD, sharing features of organization, documentation, and evaluation with SRD. The primary difference between RD and SRD is that reference data is not distributed under the authority of the Standard Reference Data Act

7. Standard Reference Data

Data that has been collected from documented sources, organized, critically evaluated using a procedure that is documented, and distributed, as described in the Standard Reference Data Act. The Standard Reference Data Act defines standard reference data as “quantitative information, related to a measureable physical or chemical property of a substance or system of substances of known composition and structure, which is critically evaluated as to its reliability under [the provisions of the Standard Reference Data Act].”⁸ Standard Reference Databases are copyrightable, and NIST may secure copyright in them.

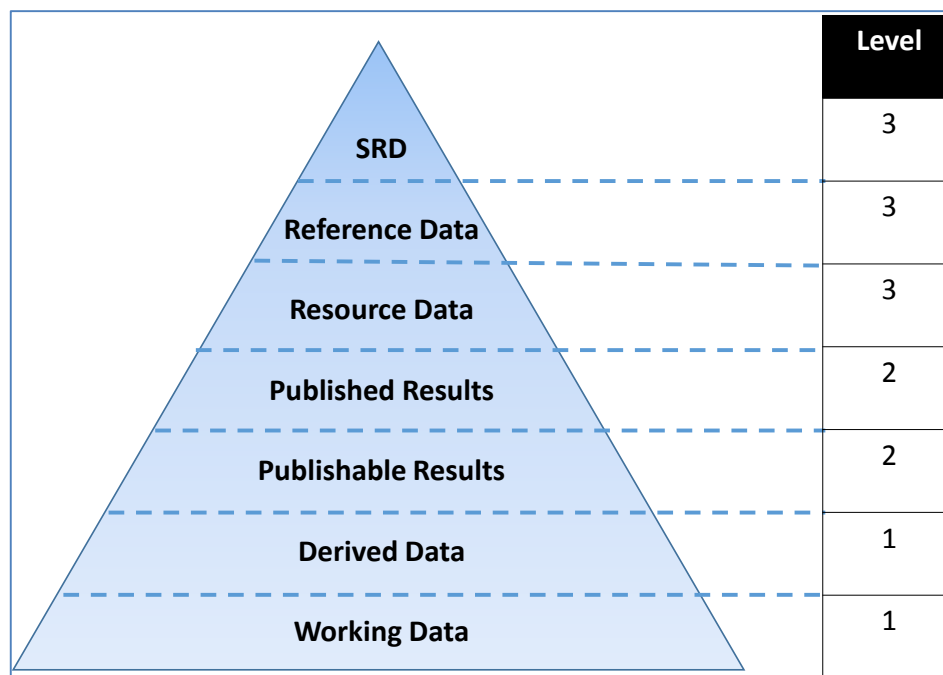
III. ACTION/CONSEQUENCE LEVELS

While the section on Data Categories is intended to define a variety of classes or grades of data that exist at NIST, this section defines corresponding requirements or consequences that should be considered when formulating data policy. As explained earlier, the purpose of this taxonomy document is not to impose these consequences or required actions on the categories, but merely to provide a vocabulary that simplifies discussion of assigning such requirements to various categories. Expressions of NIST data policy (e.g., NIST Directives, Guidance Memoranda, OU policies, etc.) should contain statements that map these consequence levels onto specific categories. Incorporating this taxonomy document as a reference into policy documents that delineate such mappings will simplify those statements of policy and reduce their ambiguity.

⁷ It should be noted that the definitions for standard reference data and reference data in this document are similar but not identical to those in the International Vocabulary of Metrology (VIM). There are two key differences: the definition of standard reference data is adopted from the SRD Act, and both definitions are broader than those in the VIM since the VIM only refers to measured data. The VIM defines reference data as being “related to a property of a phenomenon, body, or substance, or to a system of components of known composition or structure, obtained from an identified source, critically evaluated, and verified for accuracy.” The scope of reference data as used in this document expands beyond physical and chemical properties.

⁸ 15 U.S.C. § 290a, *Standard Reference Data Act*, <http://0-www.gpo.gov.librus.hccs.edu/fdsys/pkg/USCODE-1995-title15/pdf/USCODE-1995-title15-chap7A.pdf>.

Figure 2. Mapping preservation consequence levels onto the NIST data categories.



1. Preservation Consequence Levels Defined

Consistent with NIST Administrative Manual Subchapter 2.06 Records Management,⁹ the NIST Records Retention Schedule¹⁰ for Scientific and Technological Records,¹¹ and the General Records Schedule¹² for Input Records, Output Records, and Electronic Copies,¹³ the following preservation consequence levels correspond to the Data Categories in the data pyramid (*See* Figure 2):

1. No preservation requirements,
2. Individual user responsible for preservation of data,
3. Data must be backed up using a tested/automated process (i.e., proof that restoration is possible).¹⁴

⁹ <http://inet.nist.gov/mando/directives/206.cfm>

¹⁰ <http://inet.nist.gov/mando/nist-records-schedule.cfm>

¹¹ <http://inet.nist.gov/mando/services/upload/Items-25-32-Scientific-and-Technological-Records.pdf>

¹² <http://www.archives.gov/records-mgmt/grs.html>

¹³ <http://www.archives.gov/records-mgmt/grs/grs04-3.pdf>

¹⁴ The data are backed up periodically, but the backup frequency is left unspecified and commercial backup technologies such as Tivoli Storage Manager are employed, OR the data are backed up at the level of OISM Central File Services Tier 2, OR the data are backed up at the level of OISM Central File Services Tier 1.

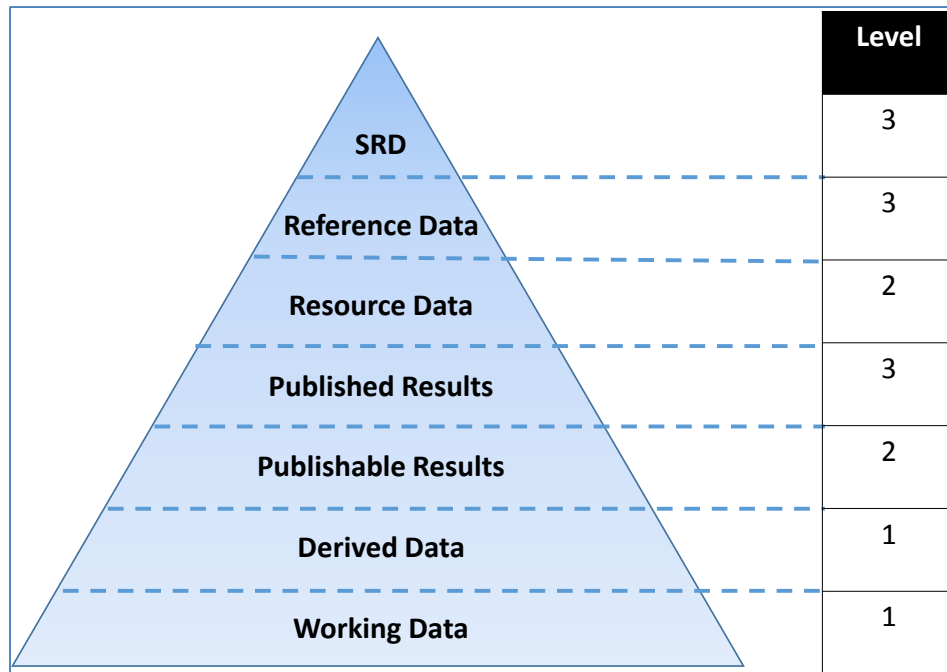


Figure 3. Mapping review consequence levels onto the NIST data categories.

2. Review Consequence Levels Defined

The following review consequence levels correspond to the Data Categories in the data pyramid (See Figure 3.):

1. No additional review requirements,
2. Technical aspects of the data must be reviewed and approved within the OU following OU policies.
3. Review by other appropriate NIST authorities (e.g., ERB, ODI) is required.

3. Discoverability Consequence Levels Defined

The following discoverability consequence levels correspond to the Data Categories in the data pyramid (See Figure 4.):

1. No discoverability requirements,
2. Metadata values must be entered into the NIST Enterprise Data Inventory (i.e., the NISTXM¹⁵ metadata) and a Persistent Identifier (PID) minted for the dataset,
3. Metadata values in the NIST Enterprise Data Inventory are made publicly accessible.

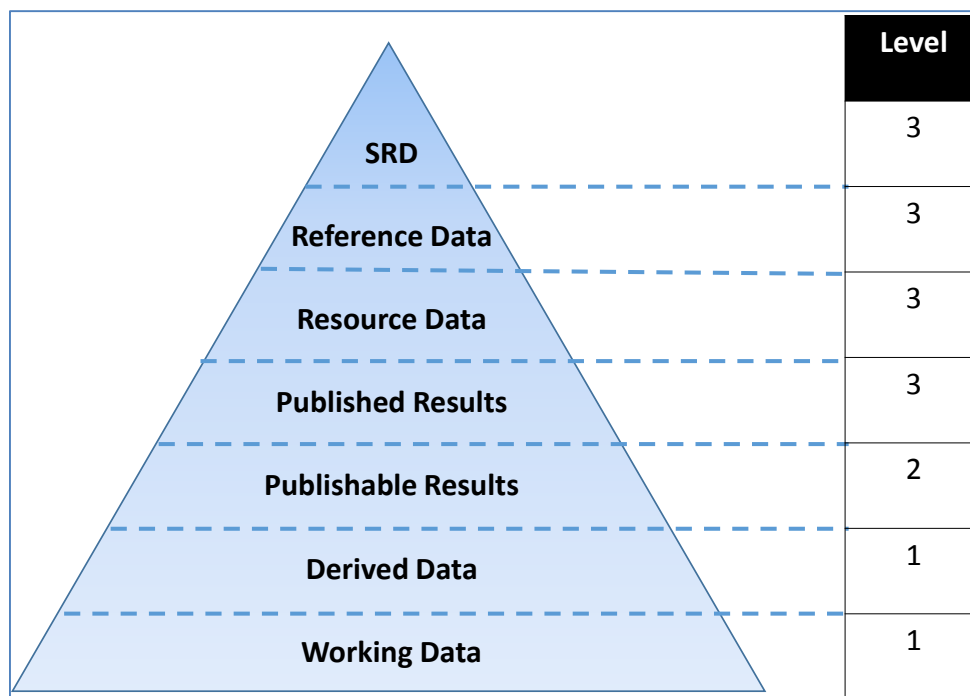


Figure 4. Mapping discoverability consequence levels onto the NIST data categories.

In addition to the guidance above, additional considerations should also be applied by each OU and Office to prioritize the availability of datasets based on factors including stakeholder need, the reasonableness of effort required to make the data available, and other relevant factors.

IV. RELEVANCE OF THE NIST IT SYSTEM SECURITY PLANS

There is a very close relationship between NIST data and the information technology (IT) systems used to store, utilize, and exchange that data. Further, extensive NIST policy governing IT systems has already been defined, and NIST has numerous special publications and Federal Information Processing Standards (FIPS) for the benefit of the nation, pursuant to the Federal

¹⁵ The NIST Extensible Metadata Schema is a definition of the minimum metadata values to be associated with NIST datasets. Formerly known as the “NIST Common Core,” the NISTXM is a very minor extension of the OMB-required Common Core metadata fields.

Information Security Management Act (FISMA) of 2002 and other legislation relative to information technology.

Federal law¹⁶ defines the three components of a widely accepted model for discussing information security, including both IT security and information assurance:

- a. **Integrity:** guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity;
- b. **Confidentiality:** preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- c. **Availability:** ensuring timely and reliable access to and use of information.

This security model applies to information, information *systems*, and related resources (including user information such as research results), and therefore is much broader than just NIST data. However, these concepts are relevant to data generated by federally funded research.

FIPS Publication 199¹⁷ defines three levels of potential impact on organizations and individuals should there be a breach of security (i.e., in this context a loss of confidentiality, integrity, or availability of the data). The potential impact can be LOW, MODERATE, or HIGH if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a severe/catastrophic effect on organizational operations, organizational assets, or individuals. These impact levels are clarified and amplified in FIPS 199. When federally funded research is intended for publication, its INTEGRITY and CONFIDENTIALITY impacts are LOW since the unauthorized modification or disclosure of the data would have a limited adverse effect on NIST operations, assets, and individuals. However, if the federally funded research contains business or personally identifiable information, proprietary information, or other sensitive information prior to publication, CONFIDENTIALITY is deemed MODERATE and therefore requires more stringent security controls. Business or personally identifiable information, proprietary information, or other sensitive information must never be published or otherwise made public. The data categorization and security controls must be documented within the respective NIST OU system security plan.

Preservation of records may be accomplished through various means. (NIST staff can see ‘How do I backup my data’ for more information.)

¹⁶ See 44 U.S.C § 3542 – Definitions.

¹⁷ FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” NIST, February 2004, available at <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	9/18/2014	Katherine Sharpless	Initial release
Rev. .01	4/13/2015	Dan Cipra	Formatting Changes Only
Rec. .02	6/18/2015	Dan Cipra	Incorporated all of the DRB changes

U.S. Designated Institutes Participating in the Mutual Recognition Arrangement (MRA) of the Comité International des Poids et Mesures (CIPM) (known as the CIPM MRA)

NIST P 5810.00
Effective Date: 10/17/2016

PURPOSE

The purpose of this directive is to define the National Institute of Standards and Technology (NIST) policy on designating other institutes for the provision of U.S. national standards.

SCOPE

This policy applies to all NIST employees involved in the provision of NIST measurement services (calibrations and reference materials) provided to customers both internal and external to NIST.

LEGAL AUTHORITIES AND REFERENCES

- [15 U.S.C. 271\(b\)](#)
- [15 U.S.C. 272\(b\) and \(c\)](#)
- Section 504 of the Foreign Relations Authorization Act 1979, codified at [22 U.S.C. 2656d\(a\)](#)
- Department Organizational Order ([DOO 30-2A](#)) National Institute of Standards and Technology
- [DOO 30-2B](#) National Institute of Standards and Technology
- [NIST P 5400.00 Measurement Quality](#)
- [NIST O 5810.00](#) Representation in CIPM and Regional Comparisons of National Standards
- NIST Quality Manual for Measurement Services, [NIST QM-I](#)
- Mutual recognition of national measurement standards and of calibration and measurement certificates issued by national metrology institutes. [CIPM MRA](#), 14 October 1999. Technical Supplement revised in October 2003 (pages 38-41)
- [NMI's and Other Designated Institutes \(Supplemental Document of the CIPM MRA\)](#)

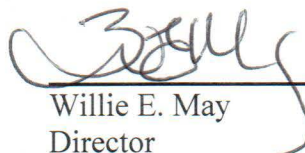
POLICY

In accordance with 15 USC 271(b), NIST is the lead national laboratory for providing measurements, calibrations, and quality assurance techniques. Under 15 USC 272(b)(2), NIST is responsible for developing, maintaining, and retaining custody of the national standards of measurement in the United States. As a general rule, NIST does not delegate this responsibility to other entities.

NIST is a signatory to the Mutual Recognition Arrangement (MRA) of the Comité International des Poids et Mesures (CIPM) as the National Measurement Institute (NMI) of the U.S. Section 6.1 of the MRA provides for cases where an NMI chooses to nominate a laboratory other than itself to be responsible for the national measurement standards relevant to that particular measurand. Under the provisions of the MRA, NIST may designate a U.S. organization other than itself to be the U.S. Designated Institute (DI) responsible for certain national measurement standards and associated services that are not covered by the activities of NIST in accordance with the terms of the MRA. Under the MRA, institutes should only be designated if they have appropriate metrological experience and scientific expertise, and: a) hold (or will hold) and maintain national measurement standards; b) will deliver metrological traceability through the provision of calibration services and/or reference materials in a well-defined metrology area, and on an equal basis to all customers; c) will act in a similar way as the NMI within a limited and well defined area of metrology, and understand and accept the obligations of participation in the CIPM MRA, and d) are appropriately resourced and sufficiently stable for their role within the national measurement system and as a DI within the CIPM MRA. *See Designated Institutes Participating in the CIPM MRA, CIPM MRA-D-06.*

NIST has reviewed the options available under the MRA and compared them to its authorization in 15 U.S.C. 272(b) and (c). NIST technical Organizational Units continually evaluate the measurement needs of the United States and the benefits to the U.S. of NIST providing those measurements. In rare instances, when a measurement is not within NIST's scope of technical expertise, NIST may select an institute for nomination to the CIPM to serve as the U.S. DI for a measurand specified by NIST if a substantial and demonstrable scientific need, trade barrier to U.S. industry, or a national security need is addressed by such designation.

The Associate Director for Laboratory Programs is responsible for ensuring the implementation of this policy.


Willie E. May
Director

10/17/16
Date

U.S. Designated Institutes Participating in the Mutual Recognition Arrangement (MRA) of the Comité International des Poids et Mesures (CIPM) (known as the CIPM MRA)

NIST O 5810.00
Effective Date: 2/7/2017

PURPOSE

The purpose of this directive is to define the process used to designate institutes other than the National Institute of Standards and Technology (NIST) for the provision of U.S. national standards.

Under the provisions of the International Committee for Weights and Measures (CIPM) Mutual Recognition Arrangement (MRA), known as the CIPM MRA, NIST (as the National Metrology Institute (NMI) of the United States) may designate a U.S. organization other than itself to be the U.S. Designated Institute (DI) responsible for certain national measurement standards and associated services that are not covered by the activities of NIST. Under the MRA, institutes should only be designated if they have appropriate metrological experience and scientific expertise, and: a) hold (or will hold) and maintain national measurement standards; b) will deliver metrological traceability through the provision of calibration services and/or reference materials in a well-defined metrology area, and on an equal basis to all customers; c) will act in a similar way as the NMI within a limited and well defined area of metrology, and understand and accept the obligations of participation in the CIPM MRA, and d) are appropriately resourced and sufficiently stable for their role within the national measurement system and as a DI within the CIPM MRA. In rare instances, when a measurement is not within NIST's scope of technical expertise, NIST may select an institute for nomination to the CIPM to serve as the U.S. DI for a measurand specified by NIST if a substantial and demonstrable scientific need, trade barrier to U.S. industry, or a national security need is addressed by such designation.

APPLICABILITY

This directive applies to NIST employees who participate in the CIPM MRA and to those involved in the provision of NIST measurement services.

REFERENCES

- [NIST P 5810.00 U.S. Designated Institutes Participating in the Mutual Recognition Arrangement \(MRA\) of the Comité International des Poids et Mesures \(CIPM\) \(known as the CIPM MRA\)](#)

REQUIREMENTS

The need for a DI for a particular measurand will be identified by a Director (or their designee) of a NIST Laboratory. That Laboratory will take on the role and responsibilities as the nominating Laboratory at NIST for the candidate DI. The Laboratory Director (or designee) will notify the NIST Measurement Services Council (NMSC).

The NIST Assessment Review Board (ARB), a subcommittee established under the NIST NMSC, will review the candidate institute's quality system and determine the institute's claimed capabilities. This may involve a visit to the institute's facilities. If deemed capable, the NMSC will advise the Associate Director for Laboratory Programs (ADLP) of their findings and recommendations.

If approved by the ADLP, the nominating NIST Laboratory will prepare a notice for publication in the Federal Register announcing to the public and interested parties that NIST has selected an institute for nomination to the CIPM to serve as the U.S. DI for a measurand specified by NIST.

The nominating NIST Laboratory will then initiate an agreement between the candidate DI and NIST. The agreement will include the following conditions and requirements. The DI will be responsible for:

- the U.S. national measurement standard(s) for a specific measurand as specified by NIST;
- disseminating standards for that measurand to U.S. industry, government, and academia;
- submitting documentation describing its quality system for review by the NIST Quality Manager and the Directors of PML and MML (or designees);
- obtaining NVLAP® accreditation with a scope that covers the intended measurement capability;
- when determined by NIST to be appropriate:
 - Participating, in partnership with NIST, in activities of the CIPM MRA;
 - Complying with the requirements of the MRA;
 - Establishing and maintaining calibration and measurement capabilities that address the scope of designation for inclusion in the Bureau International des Poids et Mesures (BIPM) Key Comparison Database; and
 - Participating in BIPM and Regional Metrology Organization Key Comparisons.

The agreement will also specify that if the DI does not meet these requirements, or if the identified scientific need or trade barrier is determined to no longer exist, NIST may revoke a DI status. A template for development of the agreement can be obtained from the Office of Chief Counsel (OCC) for NIST.

The OCC for NIST will clear the agreement and the International and Academic Affairs Office (IAAO) will receive a courtesy copy. The signed agreement will be retained by the IAAO.

When the agreement has been signed by NIST and the candidate DI, the nominating NIST Laboratory will follow the procedures listed in [CIPM MRA D-06](#), and submit the form located in Appendix I of that document in order to complete the DI nomination process and to notify the appropriate BIPM staff (see Appendix A). The nominating NIST Laboratory will provide a copy of the completed form to the IAAO. The signed document will be retained by the IAAO.

The NMSC will review the status and performance of the DI annually. If the DI does not meet the requirements as specified above or if the identified scientific need or trade barrier is determined to no longer exist, NIST may revoke a DI status.

RESPONSIBILITIES

Assessment Review Board (ARB)

- Ensures that the candidate DI's quality management system supports its measurement capability.

Associate Director for Laboratory Programs (ADLP)

- Authorizes the Laboratory Director to nominate a candidate DI.
- Authorizes the Laboratory Director to revoke the DI status,

NIST Measurement Services Council (NMSC)

- Advises the ADLP on matters regarding the candidate DI.
- Reviews the status and performance of the DI, annually.

Laboratory Directors (or their designees)

- Nominates the DI.
- Publishes a notice announcing selection of the DI in the Federal Register.
- Administers the agreement between NIST and the nominated DI.
- Provides comments received in response to the FRN to the NMSC.
- Revokes the DI status, when necessary.

Office of Chief Counsel

- Reviews and clears the agreement and the FRN.

International and Academic Affairs Office

- Retains the NIST original of the fully executed agreement and the signed CIPM MRA Nominating form.

NIST Quality Manager

- Along with members of the ARB, reviews the quality management system of the candidate DI.
- Along with members of the NMSC, reviews the status and performance of the DI.

DIRECTIVE OWNER


600 ADLP

APPENDICES

- A. Designated Institutes Participating in the CIPM MRA, CIPM MRA-D-06
- B. Revision History

APPENDIX A

DESIGNATED INSTITUTES PARTICIPATING IN THE CIPM MRA, [CIPM MRA-D-06](#) Image of the nomination form located in Appendix I of the CIPM MRA-D-06

Designated Institutes participating in the CIPM MRA CIPM MRA-D-06	
--	--

Appendix I

Nomination of a Designated Institute

Name of State/Economy: _____

Name of body that has the authority to designate: _____

Name of the institute to be designated (DI): _____

DI legal entity: _____
(if different from above)

DI Acronym: _____ DI website: _____

DI mailing address: _____

Post code: _____ City: _____ Tel/Fax: _____

Contact Person at DI: _____

Contact Person's e-mail: _____

Metrology area of designation*: _____

Note that within the meaning of the CIPM MRA, only one institute per State or Economy can be designated for any given metrology area**

We confirm that we have the authority to designate within the meaning of the CIPM MRA and this designation is compatible with the spirit, rights and obligations of the CIPM MRA and with document CIPM MRA-D-06. Furthermore we confirm that the organization being designated understands and accepts the rights and obligations of designation.

Your name and position within the designating body: _____

Date: _____ Signature: _____

Please return to:
BIPM Pavillon de Breteuil
F-92312 Sèvres Cedex, France
e-mail: cfellag@bipm.org; jcrb_es@bipm.org

* Chemistry, photometry, force, flow, volume, radioactivity, etc.

**The metrological responsibilities of Signatory NMIs and other designated institutes of the same State or Economy must always be clearly differentiated. If within a State the Signatory NMI and a DI both have responsibilities within the same metrology area, the designation scope must be specified in sufficient detail to distinguish their responsibilities. This should be done using the classification of services as available on the BIPM website at <http://www.bipm.org/utis/en/pdf/CMCs-Classification-of-services.pdf>

Note: Starting date of participation in the CIPM MRA will be considered as the date when the BIPM receives the signed designation form and it is this date that the BIPM will display.

www.bipm.org/utis/common/documents/CIPM-MRA/CIPM-MRA-D-06.pdf	Version 1 March 2015 Page 8 of 8
--	--

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	9/20/2016	Sally Bruce	Initial Draft
Rev. .01	9/21/2016	Dan Cipra	Formatting updates only
Rev. .02	12/12/2016	Sally Bruce	Updated based on DRB Comments

Calibration Services

NIST P 5900.00
Effective Date: 12/18/2015

PURPOSE

The purpose of this policy is to communicate the National Institute of Standards and Technology's (NIST's) roles and responsibilities to carry out measurement services, specifically Calibration Services. Calibration Services are performed on instruments that are metrologically suitable as reference or transfer standards and are designed to help the manufacturers and users of precision instruments achieve the highest possible levels of measurement quality and productivity. NIST Calibration Services are primarily designed to deliver measurement results with the lowest measurement uncertainty available. NIST establishes Metrological Traceability of the results and associated uncertainties of its own measurements and of results provided to customers in NIST calibration certificates and reports. These measurement results are directly linked to the System of International Units (SI) through national and international measurement standards using well-characterized, stable and predictable measurement processes.

SCOPE

This policy applies to all NIST employees involved in the provision of NIST Calibration Services provided to customers both internal and external to NIST. Unless otherwise specified, the term "Calibration Service" refers to the three types of services available, calibrations, measurement assurance programs (MAPs), and Special Tests.

LEGAL AUTHORITIES AND REFERENCES

- [15 U.S.C. 272\(b\)\(6\), \(c\)\(2\)](#). Establishment, functions, activities
- [15 U.S.C. 3710a](#). Utilization of Federal technology
- [15 CFR Part 200](#) NIST Measurement Services Policies, Services, Procedures, and Fees
- U.S. Department of Commerce Directive [DOO 30-2A](#).
- U.S. Department of Commerce Directive [DOO 30-2B](#).
- [P 5400.00 Measurement Quality Policy \(11/20/2012\)](#)
- [Calibration Service Pro Forma Invoice](#)

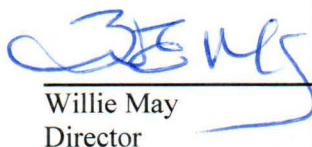
POLICY

- The calibration services of the NIST are designed to help the manufacturers and users of precision instruments achieve the highest possible levels of measurement quality and productivity. These services constitute the highest order of Calibration Services available in the United States, typically at the lowest level of measurement uncertainty. The Calibration Services provide Metrological Traceability to the System of International Units (SI). They directly link a

customer's precision equipment and transfer standards to national and international measurement standards. These services are offered to public and private organizations and to individuals.

- NIST provides Calibration Services using well-characterized, stable and predictable measurement processes. NIST calibrates instruments and devices that are metrologically suitable as reference or transfer standards.
- Calibration Services provided for entities other than U.S. Government agencies are performed under the CRADA authority (15 U.S.C. 3710a) using the [Calibration Service Pro Forma Invoice](#). Results of Calibration Services performed for entities other than agencies of the Federal government are normally treated as confidential information for a period of up to 5 years.
- Calibration Services performed for U.S. government agencies must be performed under an interagency reimbursable agreement.
- Measurement Assurance Programs (MAP) are quality control programs for calibrating a customer's entire measurement system. In a typical MAP, a stable artifact or set of artifacts called transfer standards are first measured by NIST and then sent to a customer's laboratory for a series of measurements. The transfer standards are then returned to NIST for re-measurement, along with the participating laboratory's results. NIST reports its comparative findings to the customer and, when necessary, offers guidance on achieving and maintaining measurement quality.
- Special Tests are so designated for one of the following reasons: (1) the specific type of calibration is seldom requested, thus precluding the maintenance of a large statistical base for characterizing the measurement process, or (2) the test requested is unique.

The Associate Director for Measurement Services in the Physical Measurement Laboratory is responsible for ensuring that requirements, processes and procedures are developed, implemented and maintained for the provision of the NIST Calibration Services.


Willie May
Director

12/18/15
Date

Calibration Services

NIST O 5901.00
Effective Date: 1/7/2016

PURPOSE

This order establishes requirements and responsibilities for providing NIST Calibration Services.

APPLICABILITY

This order applies to all NIST staff and management involved in the provision of NIST Calibration Services provided to customers both internal and external to NIST.

REFERENCES

- [15 U.S.C. 272\(b\), \(c\), and \(d\)](#) NIST Organic Act
- [15 U.S.C. 3710a\(c\)\(7\)\(A\) and \(7\)\(B\)](#) CRADA
- [15 U.S.C. 275\(a\) Service charges](#) and [\(c\) Fee Recovery](#)
- [15 U.S.C. 278i\(b\)](#) Justification for changes in policies and fees
- [15 CFR Part 200](#) NIST Measurement Services Policies, Services, Procedures, and Fees
- [U.S. Department of Commerce Directive DOO 30-2A](#)
- [U.S. Department of Commerce Directive DOO 30-2B](#)
- [OMB Circular No. A-25, User charges](#)
- [NIST P 5900.00 Calibration](#) (12/18/2015)
- [NIST P 5400.00 Measurement Quality Policy](#) (11/20/2012)
- [NIST N 140.01 Preparation and Clearance of Reimbursable Agreements under which NIST Provides Services to Others](#)
- [Calibration Service Pro Forma Invoice](#)
- [NIST-QM-I, NIST Quality System for Measurement Services](#)
- [NIST Administrative Manual Section 5.03 Use of the NIST Name in Advertising](#)
- [NIST Administrative Manual Section 5.16 Traceability](#)
- [NIST Administrative Manual Section 8.05 NIST Work Performed for Others](#)
- [NIST Administrative Manual Section 8.07 Working Capital Fund](#) and its [Appendix A Expense and Income Projects Reference and Guidance](#)
- [NIST Administrative Manual Section 8.11 Equipment Financing](#)

DEFINITIONS

Calibration Services are performed on devices, artifacts, and specimens intended to serve as metrological reference or transfer standards, to help manufacturers and users of measuring instruments, and of reference artifacts or materials, achieve, improve and maintain the highest possible levels of measurement quality and productivity. These services determine a relationship between indications produced by a measuring instrument or system, or between values represented by a material measure or a reference material, and the corresponding values realized by national standards. NIST's Calibration Services establish a traceability link between measured values and associated uncertainties produced by the customer's calibrated device, artifact, or specimen, and the International System of Units (SI), thus ensuring the comparability of measurement results worldwide, for use in commerce, trade, and in science and technology.

Calibration Service Pro Forma Invoice is a required legal document necessary for a non-U.S. government agency to obtain NIST Calibration Services, and contains the service terms and conditions. This legal document is a Calibration Cooperative Research and Development Agreement (C-CRADA).

Calibration Support System (CSS) is a web-based IT application and database system that provides access to NIST calibration technical, financial, and administrative data.

Intra-division Calibration Services are performed by a NIST technical division on a NIST-internal artifact or specimen that is the property of the division performing the work.

Inter-division Calibration Services are performed by one NIST technical division on a NIST-internal artifact or specimen for another NIST technical division.

Measurement Assurance Programs (MAPs) are quality control programs for calibrating a customer's entire measurement system. In a typical MAP, a stable artifact or set of artifacts called transfer standards is first measured by NIST and then sent to a customer's laboratory for a series of measurements. The transfer standards are then returned to NIST for re-measurement, along with the participating laboratory's results. NIST reports its comparative findings to the customer and, when applicable, offers guidance on achieving and maintaining measurement quality.

Memorandum of Understanding (MOU) are documents that describe a bilateral or multilateral agreement between parties which formalize a working relationship. Examples of these are Interagency Agreements (IAA) and Military Interdepartmental Purchase Requests (MIPR's). These are processes used to establish federal to federal funding agreements for Calibration Services. The NIST Office of Reference Materials receives the requests from other U.S. agencies and Department of Defense and submits the agreement packages through NIST's Reimbursable Agreements Coordination Office (RACO) for review and clearance. Once RACO approved, the Office of Reference Materials (ORM) notifies the CSS users about the funding agreement and

its availability. ORM validates folders in the CSS, monitors spending, ensures invoicing, and provides spending reports during closeouts.

Report of Calibration and Report of Test document the measurement results and corresponding uncertainties of calibrations or tests performed by NIST and apply only to the specific artifact or specimen at the time the measurements were performed unless otherwise clearly stated. Reports are the property of the customer, and copies are supplied to other parties only as required by the Calibration Service Pro Forma Invoice or requested in writing by the customer. (Note that the NIST Quality Manual, NIST-QM-I, lists information required in a Report of Calibration or Report of Test.)

Special test is either a unique or seldom-performed calibration or measurement requested by a customer (Note that special tests are covered by NIST-QM-I and the sub-level QMs).

Test Folder is clearly labeled “Test Folder” on its face and is assigned a unique Test Folder number as determined by the CSS. As a minimum the Test Folder contains the purchase order, signed Calibration Service Pro Forma Invoice or an MOU MIPR number, and a NIST 64 Record number 3 (e.g., Fee Sheet) Test folders are maintained by the Calibration Administrators in Gaithersburg and Boulder.

REQUIREMENTS

- NIST fulfills its mission in a variety of ways, including the calibration of artifacts and specimens. The NIST Calibration Services are designed to help the makers and users of precision instruments achieve the highest possible levels of measurement quality and productivity. Services directly link a customer's precision equipment or transfer standards to SI traceability through NIST scale realizations using well-characterized, stable and predictable measurement processes.
- NIST Calibration Services are provided in accordance with the NIST Policy Directive on Measurement Quality (NIST P 5400.00)
- Calibration services are performed under the authorization granted by Title 15 United States Code (U.S.C.) Section 3710a. To the extent permitted by law, NIST will protect these results from disclosure for a period of up to five years pursuant to Title 15 U.S.C. 3710a(c)(7)(A) and (7)(B).
- NIST reserves the right to decline any request for service if the work would interfere with existing commitments or priorities.
- The obligation of NIST to furnish a service is expressly limited to that which is possible with the funds provided by the customer.
- Requests for the calibration of any instrument may be declined if, in the opinion of the technical person responsible for the calibration and with the concurrence of the Group Leader, the equipment is not suitable for its intended purpose or its capabilities and features are not compatible with NIST procedures and standards.

- NIST may provide consulting, advisory, and Calibration Services for specific public entities on a reimbursable basis as long as similar requests for such services from other parties will also be honored.
- Services not offered to the public via advertisement in the SP 250 are handled as work performed for outside organizations and must follow the policies and procedures in NIST Admin Manual Subchapter 8.05, Federal Government/Non-Federal Government-Sponsored Work and CRADAs.
- NIST employees must refer inquiries to the Office of Chief Counsel (OCC) for NIST regarding NIST calibrations, tests, or other technical work related to legal actions.
- All NIST Calibration Services are provided under the C-CRADA and therefore must have a signed Calibration Service Pro Forma Invoice in place prior to the work commencing. For U.S. government agencies, a memorandum of understanding is required in lieu of the Calibration Service Pro Forma Invoice.
- C-CRADA Protected Information means the data and the Report of Calibration or Test issued by NIST will be protected from disclosure for a minimum of five (5) years. Permanent retention may be selected by the U.S. National Archives and Records Administration if the calibration service (i) becomes the subject of a Congressional investigation or comes under intensive public scrutiny or (ii) becomes involved in court decisions or legislative actions affecting the functions and activities of NIST.
- Authority to charge fees for Calibration Services, unless waived by the NIST Director when deemed to be in the interest of the government, is granted in Sections 275a and 275c of the NIST Organic Act.
- OMB Circular A-25 contains federal policy regarding fees assessed for the “sale or use of Government goods or resources” and provides the basis for setting those fees which must be sufficient to recover full costs. In addition, it requires a biennial review of fees; however, it is NIST policy to review fees annually.
- 15 USC 278i(b) requires that all changes in policies regarding fees for Calibration Services, except changes due to the costs of raw materials or of delivering calibrations services, be justified in writing by the NIST Director to the Congress. The following describes the types of funding and resources available to support NIST calibration activities. Refer to Admin Manual [Subchapter 8.02](#) for more information regarding the NIST funding structure.
- STRS appropriated funds support all research and long-term developmental work leading to the establishment and continual improvement of NIST Calibration Services. A Laboratory allocates its own STRS funding to calibration activities according to the Laboratory’s strategic priorities.
- Service Development (SD) funds support the development of future Calibration Services and improvements in existing Calibration Services. The Budget Division determines the amount of SD funds available for each Laboratory in any given year based on the NIST projected SD collections for that year, adjusted for prior-

year carryover, and on that Laboratory's share of total calibration income for the previous three years.

- Expense and Income (E&I) funds support the Laboratory's technical expenses of providing the calibration service. Refer to NIST Admin Manual [Subchapter 8.07](#), Working Capital Fund, for policies and procedures to be followed in the operation of E&I projects. Refer to NIST Admin Manual [Subchapter 8.11](#), Equipment Financing for policies and procedures in acquiring new equipment for the calibration and measurement systems.
- A Laboratory's technical costs incurred while conducting Calibration Services are charged to calibration E&I projects and reimbursed through fees that are billed to customers. These fees are either fixed or at-cost and set based on an algorithm.
- Each Laboratory establishes E&I projects for the Calibration Services it anticipates conducting during the fiscal year.
- The Calibration Services that will be charged to each E&I project are identified on Form [NIST-607](#), Request for Authorization of an Expense and Income Cost Center.
- Several similar Calibration Services may be grouped together on one E&I project. Calibration operations funds support the PML's administrative support and centralized business and information services expenses related to Calibration Services.
- Federal and non-federal government agency-sponsored work is covered by policies and procedures in NIST Admin Manual [Subchapter 8.05](#). The OCC for NIST must be consulted if circumstances arise that are not covered addressed here or Subchapter 8.05.

RESPONSIBILITIES

NIST Director

- Sets NIST policy for delivery of calibration services.

NIST Associate Director for Laboratory Programs

- Authorized by the Director to determine how the NIST calibration services policy is implemented to meet expectations.
- Ensures the implementation of notices, orders, procedures and guidance related to calibration services in the Directive Management System.
- Administers directives that ensure NIST calibration services are aligned with national priorities and needs.

PML Director

- Responsible for all procedural and process aspects of the NIST Calibration Services;

- Maintains customer, technical, and financial records related to every NIST calibration transaction via the CSS;
- Prepares and updates the SP 250 NIST Calibration Services User Guide and fee schedule appendix;
- Maintains, in consultation with the NIST Laboratories and NIST financial and legal organizations, NIST calibration administrative procedures;
- Provides, through the Calibration Administrators' team, customer interactions for incoming calibration work and record keeping/file retention of the test folders;
- Provides the necessary information, reports, and administrative support to NIST customers and Laboratories; and
- Develops, maintains, and updates the internal and external calibration websites.

Director of the Office of Reference Materials (ORM)

- Receives requests from other U.S. agencies and Department of Defense for NIST Calibration Services and establishes the federal agreement package via IAA's and MIPR's;
- Notifies the CSS users about the approved funding agreement and its availability;
- Tracks folders in the CSS for work performed under these agreements;
- Monitors spending, ensures invoicing, and provides spending reports during closeouts.
- Designs and maintains the CSS

Each NIST Laboratory Director

- Is responsible for the realization and dissemination of U.S. National Measurement Standards for specified quantities;
- Decides whether and when to offer a calibration service;
- Provides the technical and scientific work involved in the development, maintenance, and provision of Calibration Services;
- Determines the scope and estimates the level of each service;
- Establishes and maintains a quality system that assures quality in the results of its measurement services;
- Recommends annual calibration fees to ensure full cost recovery;
- Maintains records to justify calibration fees when offering measurement or Calibration Services to the public;

- Performs continuous assessment of customer needs;
- Provides customer technical support as needed; and
- Provides representation on relevant national and international committees for the technical aspects.

Statistical Engineering Division (SED) of ITL

- Provides technical assistance and guidance in the design of calibration experiments, statistical modeling, statistical computation, and statistical data analysis supporting the production of calibration results;
- Provides technical assistance and guidance in the evaluation and expression of measurement uncertainty to qualify calibrations and to assure the quality of the relationship between the calibrated device, artifact, or specimen, and national measurement standards;
- Provides training and tools to NIST staff involved in Calibration Services, and also to customers that use the calibration results, including the calibration certificates, to facilitate the use of these results taking into proper account the associated uncertainty, in support of the dissemination of national measurement standards.

Office of Financial Resource Management - Budget Division

- Reviews and approves the annual Calibrations budget as proposed by PML;
- Reviews and sets NIST-level calibration surcharge rates;
- Provides to PML the estimated cost-of-living adjustment (COLA) rate and NIST-, laboratory-, and division-level start-of-year rates for calculation of the annual calibration fees;
- Approves annual calibration fixed-fee computations for conformance to cost recovery policy; and
- Monitors expense and income activities for the Calibration Services.

Office of Financial Resource Management – Finance Division

- Handles billings and collections for all Calibration Services performed;
- Handles deferral of Service Development income in excess of expenses at year-end; and
- Serves as liaison for all financial audit activities regarding the Calibration Service activities at NIST.

Office of Facilities and Property Management - Facilities Services Division

- Receives instruments shipped to NIST for calibration;
- Delivers them to the responsible technical division, as identified on the receiving documentation; and
- Ships instruments back to customers, in accordance with packing requirements and shipping address provided by the technical division.

DIRECTIVE OWNER

600 – Associate Director for Laboratory Programs (ADLP)

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	7/1/2015	Greg Strouse (PML)	First Draft
Rev .01	7/21/2015	Dan Cipra (M&O)	Formatting updates
Rev. .02	1/8/2015	Rich Cavanagh	Updated ADLP responsibilities

Establishment of Calibration Services

NIST S 5901.01
Effective Date: 5/9/2016

PURPOSE

This directive establishes procedures for the creation of National Institute of Standards and Technology (NIST) Calibration Services. The decision to provide a new NIST calibration service requires a careful assessment of the role the service will play for NIST's customers. This suborder documents the procedures and roles and responsibilities in reaching the decision to provide a new calibration service. This applies to Regular Calibration Tests [as listed in Special Publication (SP) 250 NIST Calibration Services User Guide], Special Tests, and Measurement Assurance Programs. In this suborder, the phrase "calibration service" refers to all three types of service.

BACKGROUND

Calibrations are just one possible means of disseminating measurements and providing traceability. Considerations influencing the decision to offer a calibration service include impact of the dissemination on potential customers, demand, effectiveness and efficiency of providing the required dissemination via a calibration service (as opposed to other possible mechanisms such as SRMs, publication of test procedures or standards, or technology transfer), NIST's ability to make a long-term commitment to providing the service, life-cycle plans for the service, and the existence of a robust research program in support of the calibration service.

APPLICABILITY

This directive applies to all NIST staff and management involved in the provision of NIST Calibration Services provided to customers both internal and external to NIST.

REFERENCES

- [NIST P 5400.00 Measurement Quality Policy](#)
- [NIST P 5900.00 Calibrations Services Policy](#)
- [NIST O 5901.00 Calibration Services Order](#)

DEFINITIONS

Calibration services are performed on artifacts and specimens that are metrologically suitable as reference or transfer standards and are designed to help the manufacturers and users of precision instruments achieve the highest possible levels of measurement quality and productivity. Services directly link a customer's precision equipment or transfer standards to

the International System of Units (SI) traceability through NIST scale realizations using well-characterized, stable and predictable measurement processes.

Measurement Assurance Programs (MAPs) are quality control programs for calibrating a customer's entire measurement system. In a typical MAP, a stable artifact or set of artifacts called transfer standards is first measured by NIST and then sent to a customer's laboratory for a series of measurements. The transfer standards are then returned to NIST for re-measurement, along with the participating laboratory's results. NIST reports its comparative findings to the customer and, when necessary, offers guidance on achieving and maintaining measurement quality.

Special test is either a unique or seldom-performed calibration or measurement requested by a customer (Note that special tests are covered by NIST-QM-I and the sub-level QMs).

RESPONSIBILITIES

Physical Measurement Laboratory (PML)

- Responsible for policy and implementation of all aspects of the NIST Calibration Services;
- Maintains customer, technical, and financial records related to every NIST calibration transaction via the CSS (this must include the pro forma invoice, purchase order, business identifiable information; and may include the Report of Calibration);
- Prepares and updates the SP 250 NIST Calibration Services User Guide and fee schedule appendix;
- Maintains, in consultation with the NIST Laboratories and NIST financial and legal organizations, NIST calibration administrative procedures;
- Provides, through the Calibration Administrators' team, customer interactions for incoming calibration work and record keeping/file retention of the test folders.
- Provides the necessary information, reports, and administrative support to NIST customers and Laboratories; and
- Develops, maintains, and updates the internal and external calibration websites.

Each NIST Laboratory

- Is responsible for the realization and dissemination of U.S. National Measurement Standards for specified quantities;
- Decides whether and when to offer a calibration service;
- Provides the technical and scientific work involved in the development, maintenance, and provision of calibration services;
- Determines the scope and estimates the level of each service;

- Establishes and maintains a quality system that assures quality in the results of its measurement services;
- Recommends annual calibration fees to ensure full cost recovery;
- Maintains records to justify calibration fees when offering measurement or calibration services to the public;
- Performs continuous assessment of customer needs;
- Provides customer technical support as needed; and
- Provides representation on relevant national and international committees for the technical aspects.

Statistical Engineering Division (SED) of ITL

- Provides statistical analysis, advice, and guidance in the development of technically sound estimates of uncertainty in realizing National Measurement Standards and in the procedures used for their dissemination.;
- Provides technical guidance on the evaluation and expression of measurement uncertainty; and
- Provides training and tools to assist with statistical data analysis and uncertainty assessment for measurements and measurement systems.

PROCEDURE

The responsibility for establishing a calibration service belongs to the individual Division in which the relevant technical program resides. It is the responsibility of the individual Division to ensure that the new calibration service is in compliance with requirements of the NIST Quality System.

- In developing a new calibration service, the technical division must work with the Statistical Engineering Division of the Information Technology Laboratory to develop technically sound estimates of uncertainty.
- The responsibility for approving new calibration services resides with the PML Associate Director for Measurement Services. A Division proposing to establish a new NIST calibration service will inform the PML Associate Director for Measurement Services of the intended new service. The Division should do this early in the process of developing the new service to ensure that the proposed service does not conflict with existing or planned measurement services of other Divisions.
- Final approval of a new service requires the successful completion of a programmatic, technical, and quality review of the proposed service by the PML Associate Director for Measurement Services and the NIST Quality Manager.

A check list for the establishment of a NIST Calibration Service (See Appendix A) is available that identifies the relevant points of consideration for such a review. After the successful completion of the review, the proposing Division will submit a formal memo to the PML Associate Director for Measurement Services requesting final approval of the new service. The memo will contain the following information about the new service:

1. Proposed name of new service
2. Proposed service ID numbers
3. Official description of the service for inclusion in the NIST SP-250 calibration website
4. Technical contact for the service
5. Copy of the spreadsheet used for calculation of the calibration fees
6. Statement acknowledging the accuracy of the uncertainty calculation from the involved staff of the Statistical Engineering Division

DIRECTIVE OWNER

680 – Physical Measurement Laboratory

APPENDICES

Appendix A - Checklist for the Establishment of a NIST Calibration Service

Appendix B – Revision History

APPENDIX A

CHECKLIST FOR THE ESTABLISHMENT OF A NIST CALIBRATION SERVICE

CONTACT INFORMATION (NAME, EXTENSION, EMAIL)	
Division name and Organization Code:	
Division Chief:	Name and signature
Group Leader:	Name and signature
Quality Manager:	Name and signature
Calibration Staff:	Names
Name or Description of Proposed Service:	

CHECKLIST	COMMENTS
<input type="checkbox"/> Customer demand for the measurement service is demonstrated.	
<input type="checkbox"/> Leveraging of other NIST measurement services, other agencies' services, other NMI services, and/ or private sector offerings has been considered.	
<input type="checkbox"/> Quality assurance practices planned and identified (see NIST QM-I section 5.9).	
<input type="checkbox"/> Ability for NIST to sustain a long-term commitment to the service has been identified, and a corresponding commitment to the underpinning research has been made.	
<input type="checkbox"/> Future developments/factors that will impact the need and relevance of the service have been identified and considered.	
<input type="checkbox"/> If CMC's are planned, have they been drafted and/or submitted for review?	
<input type="checkbox"/> Description of the proposed measurement service is published with citable references, preferably as an SP-250 publication.	
<input type="checkbox"/> Uncertainty budget formulated and reviewed by Statistical Engineering Division (see Appendix C of NIST QM-I)	
<input type="checkbox"/> Quality system documentation (QM-III) is complete.	
<input type="checkbox"/> Fees for the service have been calculated/estimated.	
<input type="checkbox"/> The quality system internally reviewed at the Division level (quality and technical managers) and the NIST quality manager.	
<input type="checkbox"/> Approval memo, completed checklist, and QM-III have been sent via email to the PML Associate Director for Measurement Services with a courtesy copy sent to the NIST Quality Manager.	
<input type="checkbox"/> A visit and review by the NIST Quality Manager and PML Associate Director for Measurement Services to the facility and with its staff has been scheduled and/or arranged.	
PML Associate Director for Measurement Services	<div style="display: flex; justify-content: space-between;"> Name and signature Date </div>

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	3/4/2016	Sally Bruce	Initial draft
Rev. .01	6/2/2016	Dan Cipra	Formatting Updates only

Determining and Setting Calibration Fees

NIST S 5901.02
Effective Date: 5/9/2016

PURPOSE

This directive establishes procedures for determining and setting Calibration Fees for the provision of NIST Calibration Services.

APPLICABILITY

This procedure applies to all NIST staff and management involved in the provision of NIST Calibration Services provided to customers both internal and external to NIST.

REFERENCES

- 15 U.S.C. 272(b), (c), and (d).
- 15 U.S.C. 3710a(c)(7)(A) and (7)(B).
- 15 U.S.C. 275(a) and (c)
- 15 U.S.C. 278i(b)
- 15 CFR (b)(II)(a) 200 NIST Measurement Services Policies, Services, Procedures, and Fees
- [U.S. Department of Commerce Directive DOO 30-2A](#)
- [U.S. Department of Commerce Directive DOO 30-2B](#)
- [P 830.01 Measurement Quality Policy](#)
- [Calibration Service Pro Forma Invoice](#)
- [NIST-QM-I, NIST Quality System for Measurement Services](#)
- [NIST Administrative Manual Section 8.05 NIST Work Performed for Others](#)
- [NIST Administrative Manual Section 8.07 Working Capital Fund](#) and its [Appendix A Expense and Income Projects Reference and Guidance](#)
- [NIST Administrative Manual Section 8.11 Equipment Financing](#)
- [OMB Circular No. A-25, User charges](#)

DEFINITIONS

Calibration services are performed on artifacts and specimens that are metrologically suitable as reference or transfer standards and are designed to help the manufacturers and users of precision instruments achieve the highest possible levels of measurement quality and productivity.

Services directly link a customer's precision equipment or transfer standards to the International System of units (SI) traceability through NIST scale realizations using well-characterized, stable and predictable measurement processes.

Calibration Service Pro Forma Invoice is a required legal document necessary for a non-U.S. government agency containing the NIST calibration service terms and conditions. This legal document is a Calibration Cooperative Research and Development Agreement (C-CRADA)

Calibration Support System (CSS) is a web-based portal containing a database system that provides access to NIST calibration technical, financial, and administrative data.

Intra-division calibration services are performed by a NIST technical division on a NIST-internal artifact or specimen that is the property of the division performing the work.

Inter-division calibration services are performed by one NIST technical division on a NIST-internal device for another NIST technical division.

Measurement Assurance Programs (MAPs) are quality control programs for calibrating a customer's entire measurement system. In a typical MAP, a stable artifact or set of artifacts called transfer standards is first measured by NIST and then sent to a customer's laboratory for a series of measurements. The transfer standards are then returned to NIST for re-measurement, along with the participating laboratory's results. NIST reports its comparative findings to the customer and, when applicable, offers guidance on achieving and maintaining measurement quality.

Report of Calibration and Report of Test document the measurement results and corresponding uncertainties of calibrations or tests performed by NIST and apply only to the specific artifact or specimen at the time the measurements were performed unless otherwise clearly stated. Reports are the property of the customer, and copies are supplied to other parties only as required by the Calibration Service Pro Forma Invoice or requested in writing by the customer. (Note that the NIST Quality Manual, NIST-QM-I, lists information required in a Report of Calibration or Report of Test).

Special test is either a unique or seldom-performed calibration or measurement requested by a customer (Note that special tests are covered by NIST-QM-I and the sub-level QMs).

Test Folder is clearly labeled "Test Folder" on its face and is assigned a unique Test Folder number as determined by the CSS. As a minimum the Test Folder contains the purchase order, signed Calibration Service Pro Forma Invoice or an MOU MIPR number, and a NIST 64 Record number 3 (e.g., Fee Sheet) Test folders are maintained by the Calibration Administrators in Gaithersburg and Boulder.

RESPONSIBILITIES

Physical Measurement Laboratory (PML)

- Responsible for policy and implementation of all aspects of the NIST Calibration Services.
- Maintains customer, technical, and financial records related to every NIST calibration transaction via the CSS (this must include the pro forma invoice, purchase order, business identifiable information; and may include the Report of Calibration);
- Prepares and updates the SP 250 NIST Calibration Services User Guide and fee schedule appendix;
- Maintains, in consultation with the NIST Laboratories and NIST financial and legal organizations, NIST calibration administrative procedures;
- Provides, through the Calibration Administration team, customer interactions for incoming calibration work and record keeping of the calibration folders.
- Provides the necessary information, reports, and administrative support to NIST customers and Laboratories; and
- Develops, maintains, and updates the internal and external calibration websites.

Each NIST Laboratory

- Is responsible for the realization and dissemination of U.S. National Measurement Standards for specified quantities;
- Decides whether and when to offer a calibration service;
- Provides the technical and scientific work involved in the development, maintenance, and provision of calibration services;
- Determines the scope and estimates the level of each service;
- Establishes and maintains a quality system that assures quality in the results of its measurement services;
- Recommends annual calibration fees to ensure full cost recovery;
- Maintains records to justify calibration fees when offering measurement or calibration services to the public;
- Performs continuous assessment of customer needs;
- Provides customer technical support as needed; and
- Provides representation on relevant national and international committees.

Office of Financial Resource Management - Budget Division

- Reviews and approves the annual Calibrations budget as proposed by PML;
- Reviews and sets NIST-level calibration surcharge rates;
- Provides to PML the estimated cost-of-living adjustment (COLA) rate and NIST-, laboratory-, and division-level start-of-year rates for calculation of the annual calibration fees;
- Approves annual calibration fixed-fee computations for conformance to cost recovery policy; and
- Monitors expense and income activities for the Calibration Services.

Office of Financial Resource Management – Finance Division

- Handles billings and collections for all calibration services performed;
- Handles deferral of Service Development income in excess of expenses at year-end; and
- Serves as liaison for all financial audit activities regarding the Calibration Service activities at NIST.

PROCEDURE FOR DETERMINING FEES

Fees are set to recover the full cost of providing a calibration of a customer's instrument and include the Laboratory's direct technical costs as well as various indirect costs as described below. Whether fees are pre-determined (fixed-fee) or determined on a case-by-case basis (at-cost), the algorithm is essentially the same.

Fixed-fees are computed by the Physical Measurement Laboratory (PML) and approved by the Budget Division based on information supplied by the technical divisions and are adjusted annually to reflect any changes that may have occurred during the year. At-cost fees are determined by the technical divisions using a NIST-77, Calibration and Test Fee Computation form, and include all the items listed below except actual, rather than estimated, other objects and hours of direct labor are always used.

Calibration service fees include the following items, except as cited above:

Salary (S) {hourly rate x number of hours}
 + Leave (L) {[Sum(S)] x leave surcharge}
 + Indirect division costs (IDC) {[Sum(S) + L] x IDCR}
 + Benefits (B) {[Sum(S) + L + IDC] x benefits rate}
 = Total Direct Labor Costs (DLC)
 + Overhead (OH) {DLC x (NIST + laboratory + division + use rates)}
 + Other Objects (OO)

+ Contingency (C) $\{(DLC + OH + OO) \times \text{contingency surcharge}\}$

= Division Fee (DF)

+ PML Calibration Operations $\{DF \times \text{PML calibration operations surcharge}\}$

+ Calibration SD Surcharge $\{DF \times \text{calibration service development (SD) surcharge}\}$

= Total Fee (rounded to the nearest dollar)

a. Salary costs include the Division's technical labor hours and hourly rates spent in conducting the calibration service.

(1) At-cost fees reflect the actual salary and number of hours required for technical division personnel to provide the calibration service.

(2) Fixed-fees reflect the current actual salary (at the time the fixed-fees are prepared) and estimated number of hours required for technical division personnel to provide the service. However, fixed-fees may use an average value for the type of service involved so that the variations in actual time throughout the year will balance out. In addition, if several people work interchangeably for a variety of services, fixed-fee calculations use the pay-band salary of the "average" worker based on the total salary and total hours.

(3) All fees include the time spent in preparing the instrument for the test, the set up and check out of equipment and standards, the measurements, the data handling, and report writing.

(4) Time for direct supervision, secretarial services, or other labor may also be included in the direct labor of both at-cost and fixed-fees or, because these costs apply to all calibration services or a series of services in a division, they may be included under the indirect division costs (see item c below).

b. Leave surcharge is applied to the total salary costs for the calibration service. Admin Manual Subchapter 8.08, Appendix F, contains the current NIST leave surcharge rate.

c. Indirect division cost rate (IDCR) covers a division's costs that apply to all calibration services or a series of services in that division and are not recovered in the direct labor portion of the fee.

(1) The IDCR is applied to the calibration service's total salary and leave surcharge expenses.

(2) Appropriate costs include, for example, supervision, training, recalibration of standards, maintenance of equipment, and record keeping.

(3) The rate is determined by summing the annual labor costs of all appropriate indirect division charges and dividing by the total annual direct labor costs of all calibration services in the division that the IDC costs will support.

(4) Records of how the indirect division costs and rate are determined must be maintained by the division and should be reviewed annually to ensure cost recovery. The Division provides this information to PML annually to pass on to the Budget Division for review and approval as part of the Budget Division's review of calibration fixed-fees.

d. Benefits rate is applied to the total of the calibration service's salary, leave, and indirect division costs. Admin Manual Subchapter 8.08, Appendix F, contains the current NIST benefits rate.

e. Overhead rates include division, laboratory, and NIST overheads, as well as the use (building depreciation) surcharge, and are applied to the calibration service's total salary, leave, IDC, and benefits costs, also referred to as the total direct labor costs. Admin Manual Subchapter 8.08, Appendix F, contains the current overhead rates.

f. Other objects (itemized supplies and materials) include special items of material or equipment that are needed for each test or are supplied to the customer.

(1) At-cost fees include the actual other objects expenses incurred in providing the calibration service.

(2) Fixed-fees include the estimated other objects expenses expected to be incurred when providing the calibration service.

g. Contingency surcharge is unique to the Calibration Services and covers unanticipated fluctuations in costs, such as changes in overhead rates and pay raises, that may occur during a fiscal year for fixed-fee services or while an at-cost calibration service is being performed. The surcharge is applied to the direct labor, overheads, and other objects costs of each calibration service.

h. Calibration surcharges are unique to the Calibration Services and are applied to the division fee (labor, leave, IDC, benefits, overheads, other objects, and contingency) of both fixed-fee and at-cost calibration services in determining the total fee.

(1) Calibrations operations surcharge funds the PML calibration administrative support and centralized business and information services activities related to calibrations.

(2) Service Development (SD) surcharge recovers costs associated with the development of new or the improvement of existing calibration services. All SD funds collected are returned directly to the Laboratories.

PROCEDURE FOR SETTING FEES

Fees for services carried out at-cost are determined using [Form NIST-77](#), Calibration and Test Fee Computation form, to calculate and justify the cost of conducting the calibration service. Form NIST-77 is available online in the CSS.

Fees for each item listed in the SP 250 Appendix at a fixed-fee are established according to the following annual process and schedule for setting the predetermined calibration fees to ensure that the technical divisions are able to recover their actual costs.

PML prepares the appropriate spreadsheets by the beginning of the fiscal year for each technical division based on the previous fiscal year's (FY) fee schedule.

PML contacts the Budget Division by the beginning of the fiscal year for the estimated cost-of-living adjustment (COLA) rate, NIST-level start-of-year surcharge rates, and each Laboratory's and technical division's start-of-year overhead rates (see Admin Manual Subchapter 8.08, Cost Accounting).

PML asks the Office of Human Resources Management (OHRM) by the beginning of the fiscal year for salary data with updated pay for performance data.

OHRM provides PML with salary information within one month of the start of the fiscal year.

PML performs the necessary calculations and sends the individual spreadsheets to the technical divisions and Laboratories within two weeks of receiving all the necessary data.

The technical divisions review the spreadsheets and verify service providers, etc. and updated information is returned to PML by the first week of December.

PML prepares the final fee schedule, incorporating changes made by the Laboratories and technical divisions, and obtains additional salary information from OHRM as needed. The final fee schedule is sent to the Budget Division by the end of the second full week of December for review and approval.

The Budget Division approves the fees by the start of the new calendar year.

PML immediately informs the technical divisions and CSS Administrators and then posts the new fee schedule on the Calibration website. The PML Calibration Administrator Officer updates the fees in the CSS.

DIRECTIVE OWNER

680 – Physical Measurement Laboratory (PML)

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	3/4/2016	Sally Bruce	Initial draft
Rev. .01	6/2/2016	Dan Cipra	Formatting Updates only

Significant Changes to a NIST Calibration Service

NIST S 5901.03

Effective Date: 5/9/2016

PURPOSE

This document establishes procedures for changes to NIST Calibration Services that expand the parameter space of the measurand, change of physical location, reduce the measurement uncertainties, or significantly change methods or equipment used in the service.

APPLICABILITY

This policy applies to all NIST staff and management involved in the provision of NIST Calibration Services provided to customers both internal and external to NIST.

REFERENCES

- [P 5900.00 Calibration Services](#)
- [O 5901.00 Calibration Services Order](#)
- [P 5400.00 Measurement Quality](#)

DEFINITIONS

Calibration services are performed on artifacts and specimens that are metrologically suitable as reference or transfer standards and are designed to help the manufacturers and users of precision instruments achieve the highest possible levels of measurement quality and productivity. Services directly link a customer's precision equipment or transfer standards to the International System of Units (SI) traceability through NIST scale realizations using well-characterized, stable and predictable measurement processes.

Measurement Assurance Programs (MAPs) are quality control programs for calibrating a customer's entire measurement system. In a typical MAP, a stable artifact or set of artifacts called transfer standards is first measured by NIST and then sent to a customer's laboratory for a series of measurements. The transfer standards are then returned to NIST for re-measurement, along with the participating laboratory's results. NIST reports its comparative findings to the customer and, when applicable, offers guidance on achieving and maintaining measurement quality.

Special test is either a unique or seldom-performed calibration or measurement requested by a customer (Note that special tests are covered by NIST-QM-I and the sub-level QMs).

RESPONSIBILITIES

Physical Measurement Laboratory (PML)

- Responsible for policy and implementation of all aspects of the NIST Calibration Services.
- Maintains customer, technical, and financial records related to every NIST calibration transaction via the CSS (this must include the pro forma invoice, purchase order, business identifiable information; and may include the Report of Calibration);
- Prepares and updates the SP 250 NIST Calibration Services User Guide and fee schedule appendix;
- Maintains, in consultation with the NIST Laboratories and NIST financial and legal organizations, NIST calibration administrative procedures;
- Provides, through the Calibration Administrators' team, customer interactions for incoming calibration work and record keeping/file retention of the test folders;
- Provides the necessary information, reports, and administrative support to NIST customers and Laboratories; and
- Develops, maintains, and updates the internal and external calibration websites.

Each NIST Laboratory

- Is responsible for the realization and dissemination of U.S. National Measurement Standards for specified quantities;
- Decides whether and when to offer a calibration service;
- Provides the technical and scientific work involved in the development, maintenance, and provision of calibration services;
- Determines the scope and estimates the level of each service;
- Establishes and maintains a quality system that assures quality in the results of its measurement services;
- Recommends annual calibration fees to ensure full cost recovery;
- Maintains records to justify calibration fees when offering measurement or calibration services to the public;
- Performs continuous assessment of customer needs;
- Provides customer technical support as needed; and
- Provides representation on relevant national and international committees for the technical aspects.

Statistical Engineering Division (SED) of ITL

- Provides statistical analysis, advice, and guidance in the development of technically sound estimates of uncertainty in realizing National Measurement Standards and in the procedures used for their dissemination;
- Provides technical guidance on the evaluation and expression of measurement uncertainty; and
- Provides training and tools to assist with statistical data analysis and uncertainty assessment for measurements and measurement systems.

PROCEDURE

Changes to NIST calibration services should be a natural outcome of continual improvements to NIST services. The following describes the process and identifies the roles and responsibilities in reviewing and approving official changes to established NIST calibration services that result in changes to the capabilities listed in the SP-250 NIST Calibration Services User Guide, and/or changes requiring modification to the NIST Calibration and Measurement Capabilities (CMCs) listed in the BIPM Key Comparison Database (KCDB). This procedure applies to Regular Calibration Tests [as listed in Special Publication (SP) 250 NIST Calibration Services User Guide], Special Tests, and Measurement Assurance Programs. The phrase “calibration service” refers to all three types of service.

The responsibility for improving a calibration service belongs to the individual Division in which the relevant calibration service resides. If the change to the service results in a significant change to the published uncertainties of a service, the technical Division must work with the Statistical Engineering Division of the Information Technology Laboratory to determine the new technically sound estimates of uncertainty. The responsibility for approving a significant change to a calibration service resides with the Leader of the relevant Group.

Upon approval of a change to an established calibration service by the Group Leader, they will electronically submit a memo describing the changes and any affected CMCs to the relevant Division Chief, the PML Associate Director for Measurement Services, and the NIST Quality Manager. The PML Associate Director for Measurement Services will forward the approved changes so that the required changes are made to the NIST calibration website.

It is the responsibility of the calibration staff to ensure that all changes to a calibration service are reported in the Division Quarterly Quality Report. It is the responsibility of the individual Division to ensure that the changes to the calibration service are in compliance with requirements of the NIST Quality System, and thereby is reflected in the appropriate QM-III or sub-level quality manual. Additionally, if the changes need to be reflected in the NIST CMCs, it is the responsibility of the calibration staff to initiate and orchestrate the CMC approval process.

The memo will contain the following information about the calibration service:

1. Name of new service

2. Service ID numbers
3. Official description of the service (if changed) for inclusion in the NIST calibration website and SP 250 Appendix – Fee Schedule
4. Technical contact, Group Leader, Report signatory for the service
5. Statement acknowledging the uncertainty calculations from the involved staff of the Statistical Engineering Division
6. Signed copy of the Checklist for the Establishment of a New Calibration Service found in S 5901.01 (Establishment of a Calibration Service).

DIRECTIVE OWNER

680 – Physical Measurement Laboratory (PML)

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	3/4/2016	Sally Bruce	Initial draft
Rev. .01	6/2/2016	Dan Cipra	Formatting Updates only

Termination of Calibration Service

NIST S 5901.04

Effective Date: 5/9/2016

PURPOSE

This directive establishes procedures for the termination of a NIST Calibration Service.

APPLICABILITY

This policy applies to all NIST staff and management involved in the provision of NIST Calibration Services provided to customers both internal and external to NIST.

REFERENCES

- [P 5900.00 Calibration Services](#)
- [O 5901.00 Calibration Services Order](#)
- [P 5400.00 Measurement Quality](#)

DEFINITIONS

Calibration services are performed on artifacts and specimens that are metrologically suitable as reference or transfer standards and are designed to help the manufacturers and users of precision instruments achieve the highest possible levels of measurement quality and productivity. Services directly link a customer's precision equipment or transfer standards to the International System of Units (SI) traceability through NIST scale realizations using well-characterized, stable and predictable measurement processes.

Measurement Assurance Programs (MAPs) are quality control programs for calibrating a customer's entire measurement system. In a typical MAP, a stable artifact or set of artifacts called transfer standards is first measured by NIST and then sent to a customer's laboratory for a series of measurements. The transfer standards are then returned to NIST for re-measurement, along with the participating laboratory's results. NIST reports its comparative findings to the customer and, when necessary, offers guidance on achieving and maintaining measurement quality.

Special test is either a unique or seldom-performed calibration or measurement requested by a customer (Note that special tests are covered by NIST-QM-I and the sub-level QMs).

RESPONSIBILITIES

Physical Measurement Laboratory (PML)

- Responsible for policy and implementation of all aspects of the NIST Calibration Services.
- Maintains customer, technical, and financial records related to every NIST calibration transaction via the CSS (this must include the pro forma invoice, purchase order, business identifiable information; and may include the Report of Calibration);
- Prepares and updates the SP 250 NIST Calibration Services User Guide and fee schedule appendix;
- Maintains, in consultation with the NIST Laboratories and NIST financial and legal organizations, NIST calibration administrative procedures;
- Provides, through the Calibration Administrators' team, customer interactions for incoming calibration work and record keeping/file retention of the test folders.
- Provides the necessary information, reports, and administrative support to NIST customers and Laboratories; and
- Develops, maintains, and updates the internal and external calibration websites.

Each NIST Laboratory

- Is responsible for the realization and dissemination of U.S. National Measurement Standards for specified quantities;
- Decides whether and when to offer a calibration service;
- Provides the technical and scientific work involved in the development, maintenance, and provision of calibration services;
- Determines the scope and estimates the level of each service;
- Establishes and maintains a quality system that assures quality in the results of its measurement services;
- Recommends annual calibration fees to ensure full cost recovery;
- Maintains records to justify calibration fees when offering measurement or calibration services to the public;
- Performs continuous assessment of customer needs;
- Provides customer technical support as needed; and
- Provides representation on relevant national and international committees for the technical aspects.

PROCEDURE

The decision to terminate a NIST calibration service requires a careful assessment of the role the service plays for NIST's customers and of the potential impact of the termination. Any termination plan must provide reasonable alternatives to current customers of the NIST calibration service proposed for termination. Thus, all termination plans should be prepared in close cooperation with key NIST customers, preferably far in advance of any termination dates with a goal of providing a more effective means traceability. In addition, one should consider and determine if the potential terminated service is incorporated or referenced within a regulation or requirement of another US Government agency (e.g., DOD, EPA, DOE, HHS, and DHS are a few examples).

The following policy documents the procedures and roles and responsibilities in reaching such a decision. This policy applies to Regular Calibration Tests [as listed in Special Publication (SP) 250 NIST Calibration Services User Guide], Special Tests, and Measurement Assurance Programs. In this policy, the phrase "calibration service" refers to all three types of service.

The responsibility for terminating calibration services belongs to the individual Division in which the relevant calibration service resides. The responsibility for final approval of a proposed termination resides with the PML Associate Director for Measurement Services. A Division proposing to terminate a NIST calibration service will inform the PML Associate Director for Measurement Services of the intended termination plans. The Division should do this early in the planning process so that the PML Associate Director for Measurement Services may assess the impact of such plans on other NIST programs.

The Division has the responsibility of assessing the impact of a proposed termination. Accordingly, the Division should notify customers of the last five years to inform them of the proposed service termination, proposed alternatives for customers, and solicit feedback, comments, concerns, and questions. Three months should elapse to collect customer responses. The text of the notification must be approved by the PML Associate Director for Measurement Services with a cc to the NIST Quality Manager before distribution.

After analysis of the feedback from the notified customers, the Division should make a final decision regarding their intent to terminate the service. The Division will make a short presentation to the PML Associate Director for Measurement Services and NIST Quality Manager stating the proposed final decision, a summary of the comments from customers, alternatives provided to the customers (if necessary), and a timeline if termination is proposed. The PML Associate Director for Measurement Services will then determine if termination of the service is in the best interests of NIST and the customers.

Service termination should not take effect until at least one year after the Laboratory has notified the affected parties.

A memo to the PML Associate Director for Measurement Services with a cc to the NIST Quality Manager proposing termination of a service may be sufficient if a service has had no customers in the last five years.

DIRECTIVE OWNER

680 – Physical Measurement Laboratory

APPENDICES

A – Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	3/4/2016	Sally Bruce	Initial draft
Rev. .01	6/2/2016	Dan Cipra	Formatting Updates only

Information Systems Management and Use Policy

NIST P 6100.00
Effective Date: 4/3/2014

PURPOSE

The purpose of this directive is to articulate NIST's commitment in carrying out its mission by utilizing effective, efficient, and secure information system (IS) resources.

SCOPE

This policy applies to information system resources used in the conduct of NIST business.

LEGAL AUTHORITY AND REFERENCES

- Department of Commerce (DOC) Information Technology Portfolio Management Policy
- [Department Organization Order \(DOO\) 30-2B](#), Section 6.04, The Office of Information Systems Management
- [OMB Circular No. A-130 Revised](#), Memorandum for Heads of Executive Departments and Agencies on Management of Federal Information Resources
- Clinger-Cohen Act (also known as "[Information Technology Management Reform Act of 1996](#)"), Public Law (P.L.) 104-106, Division E
- [E-Government Act of 2002](#), Public Law (P.L.) 107-347

DEFINITIONS

NIST Information System - A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual, which are under the same direct management control and share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals to support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, cloud service provider, or shared information processing service organization (IPSO).

NIST Information System User – Any NIST employee or associate who enters into an agreement with NIST, permitting their use of NIST Information System resources.

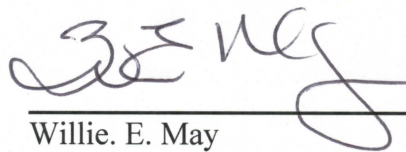
POLICY

It is NIST policy to implement and manage information system resources, including access to and use of such resources, in accordance with:

- DOC and NIST-wide directives, to include suborders, governing the effective, efficient, and secure utilization of information system resources, including capital planning and investment, budgeting, privacy, strategic planning, and acquisition strategy and performance measures;
- The NIST-wide enterprise architecture and technical reference model, including standards by which services and infrastructure must be provided; and
- Department-wide information system initiatives and strategies collaboratively developed by the NIST Chief Information Officer (CIO) and the Department of Commerce CIO.

The NIST CIO is responsible for defining requirements, processes, and procedures and establishing the enterprise architecture and reference model standards to manage information systems used in the conduct of NIST business.

Supervisors and Associate Hosts (as defined in the NIST Associate Information System) are responsible for ensuring that NIST information system users are made aware of all requirements associated with access and use of NIST information systems.



Willie. E. May
Director

7/24/15
Date

Employee-Issued Computing and Telecommunication Devices

NIST N 6100.01
Effective Date: 11/21/2012

PURPOSE

This directive establishes controls to ensure that the National Institute of Standards and Technology (NIST) does not pay for unused or underutilized information technology (IT).

APPLICABILITY

This directive applies to all NIST employees and associates.

REFERENCES

- [Executive Order 13589, “Promoting Efficient Spending” \(11/9/2011\)](#)
- Email from DOC CIO entitled “Bureau Plans to Promote Efficient Spending on Employee-Issued Devices” dated November 22, 2011

BACKGROUND

Executive Order 13589 requires Federal agencies to establish controls to ensure that they are not paying for unused or underutilized IT by limiting the number of IT devices (e.g. mobile phones, smartphones, desktop and laptop computers, and tablet personal computers) issued to employees, consistent with the Telework Enhancement Act of 2010 (P.L. 111-292), operational requirements (including continuity of operations), and initiatives designed to create efficiency through the effective implementation of technology.

REQUIREMENTS

This directive governs the number of Federal government owned computing and telecommunications devices assigned in the NIST Property System to a Federal employee as the Contact or Custodian for use by that employee (e.g., laptops, desktops, PDA/smartphones, tablets) for general use (e.g., email, internet access, word processing).

This directive does not apply to:

- Devices directly connected to laboratory equipment or needed to remotely control such equipment
- Devices used for specialized computation, data collection, or research
- Devices shared by multiple people (e.g. servers, loaner laptops, training room computers)
- Devices kept in reserve for the repair or replacement of failed units
- Devices needed to test or pilot the introduction and support of new technology and services

- Devices needed to support infrastructure, services, or continuity of operations

Devices assigned to a Federal employee in the NIST Property System for loan to a NIST associate shall not count against the devices issued to the employee for their own use, but will count against the devices assigned to the associate.

Based on the operational needs of NIST, each employee shall have assigned individually to them for their own use, and each associate will have loaned to them for their own use:

- No more than two of the following:
 - One desktop computer;
 - One laptop computer; or
 - One tablet computing device
- No more than one of the following:
 - Cell phone
 - Smartphone

EXCEPTIONS

Organizational Units (OUs) may deviate from this directive by documenting their own policy in writing. The policy must include an explanation of the reason for the variance from this directive. The policy must be signed by the OU Director with signed concurrence of the Associate Director for the OU. A copy of the policy shall be forwarded to the NIST Chief Information Officer (CIO).

Individual exceptions (from the NIST directive if no OU policy exists, or from the OU policy if one exists) must be documented by a written justification approved by the user's supervisor and kept on record by the OU.

RESPONSIBILITIES

Associate Directors –

- Review and concur with any individual OU policy for those OUs under their area of responsibility (see Exceptions paragraph above).

OU Directors –

- Evaluate situation with respect to OU mission and determine if a separate OU policy that deviates from this directive is needed.
- Obtain concurrence of the Associate Director for the OU if separate OU policy is created.
- Forward copy of OU policy to the NIST CIO if one is created.

Office of Information Systems Management –

- Maintain a copy of the OU policy provided by each OU that sets its own policy.
- Review OU policy and if not in agreement with the explanation for the variance from this directive, work with the subject OU to adjust the OU policy as needed.

NIST Supervisors –

- Issue written individual exceptions from this NIST directive if needed.
- Ensure written copies of any individual exceptions from this NIST directive are kept on file within their OU.

All NIST employees and associates –

- Comply with the requirements specified in this directive.

DIRECTIVE OWNER

180 - Office of Information Systems Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	9/20/12	Susannah Schiller	Initial Draft
Ver 0.1	9/20/12	Dan Cipra	Reformatted text
Ver 0.2	9/21/12	Susannah Schiller	Edited applicability and responsibilities
Ver 0.3	9/27/12	Bruce Rosen	Corrected misspelling
Ver 0.4	10/15/12	Bruce Rosen	Update based on comments from Deputy Chief Counsel for NIST
Ver 0.5	10/18/12	Bruce Rosen	Update based on additional comments from Deputy Chief Counsel for NIST
Ver 0.6	10/23/12	Bruce Rosen	Update based on additional comments from Deputy Chief Counsel for NIST and discussion with Deputy CIO
Ver 0.7	10/25/12	Dan Cipra	Accepted all changes/comments and prepared for DRB review.
Ver 0.8	10/25/12	Bruce Rosen	Updated based on comments from DRB review.
Ver 0.9	11/07/12	Bruce Rosen	Hyperlink added to Reference..
Ver 0.9a	11/8/12	Dan Cipra	Updated OU Internal Policy
Ver 0.10	11/13/12	Bruce Rosen	Updated based on comments during DRB meeting of 11/13/2012.
Ver. 1.0	11/14/12	Dan Cipra	Final edits accepted.

Network, Boundary Protection

NIST S 6102.01

Issue Date: 9/25/2014

Effective Date: 12/03/2007

PURPOSE

The purpose of this directive is to define requirements for NIST network boundary protection in support of NIST programs.

APPLICABILITY

These requirements apply to all NIST information system resources used in the conduct of NIST business.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Access Control (AC), Security Assessment and Authorization (CA), and System and Communication Protection (SC) families.

DEFINITIONS

- Network security zone: Segment of a NIST network that is defined by common security policies, i.e., internal and external network security zones.
- Internal network security zone: NIST network security zones without direct access from the Internet or networks not owned by NIST.
- External network security zone: NIST network security zones with direct access from the Internet or network not owned by NIST.

REQUIREMENTS

1. Servers shall never be connected to multiple network security zones or the Internet and a NIST security zone simultaneously.
2. Computers shall only connect to network security zones if they meet security requirements specified for that network security zone.

3. Servers shall connect management network interfaces and general use network interfaces (i.e., to include virtual) to different network security zones as long as there is adequate system controls restricting logical access between these interfaces and as approved by the NIST IT Security Officer (ITSO).
4. Network traffic entering or leaving a network security zone shall have source addresses that are consistent with the network addresses assigned on each side of the network security zone.
5. Network traffic that has private IP addresses or RFC1918 (i.e., Address Allocation for Private Internets) reserved addresses shall not be transmitted between NIST networks and the Internet.
6. Network traffic originating from the Internet, or other network not owned by NIST, shall authenticate through computers in external network security zones. Access to the internal network security zones will only be allowed through the external security zones unless otherwise approved by the NIST ITSO.
7. Network traffic passing through network security zones shall be monitored with an Intrusion Detection System (IDS) or by an Intrusion Prevention System (IPS).
8. OISM managed network firewalls shall have documented rules that define the types of traffic allowed between each set of interfaces. These rules and any changes to these rules shall be approved by the NIST ITSO (or designee). The rules shall restrict traffic to only that which is necessary for work-related IT operations.
9. Internal network security zones may share internal network components supporting, and logically segmented, from other internal network security zones.
10. Internal network security zones shall be segmented from other internal network security zones using network firewall, network access control list, or a technical equivalent approved by the NIST ITSO.
11. External network security zones, shall not be supported by network components (e.g., routers and switches) supporting internal network security zones unless approved by the NIST ITSO.
12. External network security zones and internal network security zones shall be segmented and protected by network firewalls managed by the Office of Information Systems Management (OISM).
13. Network firewalls shall not be configured to allow all external IP addresses to send packets to all internal IP addresses, even if such activity is restricted to certain ports. In firewall terminology, the firewall policy shall not contain "Inbound Any Any Allow" rules.
14. Network firewalls shall operate in a fail-closed configuration.

DIRECTIVE OWNER

18 - [Office of Information Systems Management](#)

Basic Input/Output System (BIOS)

NIST S 6102.04

Issue Date: 9/25/2014

Effective Date: 08/16/2012

PURPOSE

The purpose of this directive is to define requirements for BIOS in support of NIST programs.

APPLICABILITY

This directive applies to all NIST-owned computers with Microsoft Windows XP or Windows 7 that connect to NIST networks or the Internet. This includes computers with multiple platforms (i.e., multi-boot) where at least one of the platforms is Windows XP or Windows 7. This does not include non-Windows computers running Windows XP or Windows 7 virtual machines. The scope will be expanded to include other platforms as BIOS protection becomes available for those platforms. This directive does not apply to non-networked computers (e.g., "stand-alone" laboratory equipment) and non-NIST-owned computers.

REFERENCES

- [NIST Special Publication 800-147 "BIOS Protection Guidelines"](#)
- [Department of Homeland Security \(DHS\) Federal information System Memo \(FISM\) \(DHS FISM 12-01\)](#)

This Directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."](#) Configuration Management (CM) and System Information Integrity (SI) families.

REQUIREMENTS

1. All computers must have a protected and signed BIOS installed and enabled by August 31, 2014.
2. All computer deployments must be coordinated with the Operating Unit IT Security Officer (OU ITSO).

3. Only Windows XP computers with enabled, protected and signed BIOS may be upgraded.
4. All computer purchases must include protected and signed BIOS.
5. Waiver requests for these requirements must follow procedures located at:
https://inet.nist.gov/oism/howdoi/iss_waivers.cfm.

DIRECTIVE OWNER

18 - [Office of Information Systems Management](#)

Network, External Connections

NIST S 6102.06

Issue Date: 9/25/2014

Effective Date: 04/29/2013

PURPOSE

To define requirements for the use of external networks connected to NIST networks in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system resources used in the conduct of NIST business. This directive does not apply to remote access connections or mobile Internet broadband services.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Security Assessment and Authorization (CA) and System and Communications Protection (SC) families;
- [OMB Memorandum 08-05, "Implementation of Trusted Internet Connections;"](#) and
- [OMB Memorandum 09-32, "Update on the Trusted Internet Connections Initiative"](#)

REQUIREMENTS

1. The direct connection of external networks, including Internet services, point-to-point data network circuits, wide area networks, and permanent virtual private networks (VPNs) with NIST networks must be operated and managed by the Office of Information Systems Management (OISM).
2. All Internet services must be compliant with OMB TIC requirements.
3. Waiver requests for these requirements must follow procedures located at: https://inet.nist.gov/oism/howdoi/iss_waivers.cfm.

DIRECTIVE OWNER

18 - [Office of Information Systems Management](#)

Network, Wireless Security (IEEE 802.11)

NIST S 6102.07

Issue Date: 9/25/2014

Effective Date: 08/30/2012

PURPOSE

To define requirements which ensure that the Institute of Electrical and Electronic Engineers (IEEE) 802.11 (Wi-Fi) wireless local area networking (WLAN) technology is deployed and used securely in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users and all NIST information system resources used in the conduct of NIST business.

Requirements for use of off-campus remote access to NIST wireless networks (e.g., home wireless networks) are outside the scope of this directive.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Information Technology Requirements, CITR-014 Wireless Encryption Enhancements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Access Control (AC) family.

REQUIREMENTS

Wireless Network Management

1. Wireless networks must be configured and managed to align with NIST SP 800-97, and NIST SP 800-153. Deviations must be documented in an approved System Security Plan.
2. Wireless networks connected in any way to NIST wired networks operated and managed by the NIST Office of Information Systems Management (OISM) must be operated and managed by OISM.
3. Wireless networks not connected to NIST wired networks must be registered and follow registration requirements defined in the NIST WI-FI Registration and Waiver request template.

- Wireless networks must be registered and approved before becoming operational. Existing wireless networks must be registered immediately but may continue operating while the registration request is being considered.
 - Systems that are not managed by OISM require registration with OISM.
4. Waiver requests for these requirements must follow procedures located at:
https://inet.nist.gov/oism/howdoi/iss_waivers.cfm

Wireless Network Access

1. Only authorized users and devices are permitted to connect to NIST wireless networks.
2. Only authorized and registered NIST visitors are permitted access to the NIST-Visitor wireless network or any wireless networks authorized for visitor access.
3. Only authorized NIST employees and associates are permitted access to the NISTNet wireless network or any other wireless networks authorized for NIST users.
4. Connecting simultaneously to a wireless network and any other network which is physically or logically separated by a firewall or equivalent control is prohibited.
5. Connecting simultaneously to the NISTNet wireless network and a completely isolated network (i.e., physically separated from any other network) is prohibited.
6. Devices with wireless network interfaces must not use "wi-fi" ad hoc mode while connected to any NIST networks.

DIRECTIVE OWNER

18 - [Office of Information Systems Management](#)

Vulnerability Scanning

NIST S 6102.09

Issue Date: 9/25/2014

Effective Date: 7/2/2013

PURPOSE

The purpose of this directive is to define requirements for vulnerability scanning in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system resources used in the conduct of NIST business, including those which are operating in isolation from the NIST network (i.e., air-gapped networks).

These requirements also apply to all information systems owned or operated on behalf of NIST where NIST has the legal and/or contractual authority to dictate requirements.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Risk Assessment (RA), and System and Information Integrity (SI) families.

REQUIREMENTS

1. All networked devices must be scanned for known vulnerabilities in accordance with [CITR-016](#).
2. All web servers and web applications must be scanned for known vulnerabilities at least annually.
3. New web applications, or those existing web applications undergoing a significant change, must be scanned for known vulnerabilities before becoming operational.

4. Vulnerability scanning must be conducted using NIST IT Security Officer (ITSO) approved tools managed by the Office of Information Systems Management (OISM).
5. No other vulnerability scanning is permitted without authorization from the NIST ITSO.

DIRECTIVE OWNER

18 - [Office of Information Systems Management](#)

Cybersecurity Workforce

NIST S 6102.13

Issue Date: 2/24/2016

Effective Date: 2/24/2016

PURPOSE

This suborder defines the cybersecurity code that must be used for roles deemed significant in terms of information systems security. The cybersecurity code is derived from the National Cybersecurity Workforce Framework, and is used to identify incumbents or positions for which the primary function is cybersecurity.

APPLICABILITY

This suborder is applicable to positions (i.e., roles) deemed significant in terms of information system security, as defined in [Commerce Interim Technical Requirement \(CITR\) – 006](#).

The cybersecurity codes are only applicable to operational positions (i.e., research positions are not coded).

REFERENCE

- [OPM Guide to Data Standards, Part A: Human Resources](#),
- [NIST Cybersecurity Workforce Framework](#),
- This Directive is supplemental to a suite of security controls consisting of:
 - NIST information security Directives;
 - [Commerce Interim Technical Requirements](#);
 - [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
 - [NIST Special Publication 800-53](#), “Security and Privacy Controls for Federal Information Systems and Organizations”, Personnel Security family.

DEFINITIONS

Cybersecurity Specialty Area – a position or incumbent’s primary work function involving cybersecurity

Cybersecurity Specialty Area Code – two digit code defined in OPM Guide to Data Standards, Part A: Human Resources, used to identify incumbents or positions for which the primary function is cybersecurity

ACRONYMS

ACS – Automated Classification System

APMS – Alternative Personnel Management System

NAIS – NIST Associate Information System

PD – position description

REQUIREMENTS

1. NIST Hiring Managers must ensure review and inclusion of the cybersecurity code in position descriptions and on form CD-516, Classification and Performance Management Record, for the roles defined below.
2. NIST Sponsors of Associates must ensure review and inclusion of the cybersecurity code in the NIST Associate Information System (NAIS), for the roles defined below, when functionality becomes available.

Information System Security Role	Cybersecurity Specialty Area	Cybersecurity Specialty Area Description
Chief Information Officer, Authorizing Official, or Information System Owner (ISO)	90 NOTE: Where an individual is in a role that is non-supervisory, the 75 code shall be used.	Cybersecurity Supervision, Management, and Leadership - Supervises, manages, and/or leads work and workers performing cybersecurity work (i.e., the work described in the Categories and Specialty Area codes with values 10-75).
NIST and OU level Information Technology Security Officer (NIST and OU ITSO)	74 NOTE: Where an individual is in a role supporting 74 and 72 or 54, the 74 code shall be used.	Security Program Management (Chief Information Security Officer [CISO]) - Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
Information System Security Officer (ISSO)	72 NOTE: Where an individual is in a role supporting both 72 and 53 or 54, the 72 code shall be used.	Information Systems Security Operations (Information Systems Security Officer [ISSO]) - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.
Incident Responders (IR)	53	Incident Response - Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and

		response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
Security Control Assessor (SCA)	54	Vulnerability Assessment and Management - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

ROLES AND RESPONSIBILITIES

NAIS System Owner(s)

- facilitate updating positions with codes
- integrate cybercodes into associate processes
- ensure codes are present in the NAIS
- collaborate with OISM to periodically review

Office of Human Resource Management

- facilitate updating positions with codes
- integrate cybercodes into hiring and position classification processes
- ensure codes are present in the ACS, and in individual position descriptions
- collaborate with OISM to periodically review

Office of Information Systems Management

- maintain inventory of roles
- collaborate with OHRM and NAIS System Owners to periodically review

DIRECTIVE OWNER

18 - [Office of Information Systems Management](#)

APPENDICES

A. Revision History

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Created	1/6/2016	Carolyn Schmidt	Initial draft
Rev. .01	2/19/2016	Dan Cipra	Formatting updates only

Information System Vulnerability Management

NIST S 6102.15

Issue Date: 3/30/2016

Effective Date: 3/30/2016

PURPOSE

Vulnerability scanning of National Institute of Standards and Technology (NIST) information systems is conducted in accordance with NIST directive on Vulnerability Scanning, and remediated based on Commerce Information Technology Requirement (CITR-016), Vulnerability Scanning and Patch Management. The purpose of this directive is to define how vulnerabilities are categorized based on severity of risk to NIST information systems, such that higher risk vulnerabilities are provided consistent priority.

APPLICABILITY

This Directive applies to operational internal (non-public) and external (public) networked systems and web applications. This Directive also applies to new systems in development and those systems undergoing modifications. Secure configurations requirements are described in the NIST [Secure Configurations Directive](#).

REFERENCE

This Directive is supplemental to a suite of security controls consisting of:

- [NIST information security Directives](#);
- [Commerce Interim Technical Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Risk Assessment \(RA\) and System and Services Acquisition \(SA\) families](#).

DEFINITIONS

Assessment & Authorization – process administered by OISM in which information system controls are assessed, identified risks are reviewed with management, and systems are formally authorized to operate.

Vulnerability Severity – priority assigned to an active, identified vulnerability (Informational, Low, Medium, High, or Critical) which is derived from various sources, such as the CVSS, OS or application vendor, or scanning product vendor. Priority may be elevated to Critical by the NIST ITSO based on various vulnerability attributes, such as a vendor designating a vulnerability as Critical, or if a vulnerability could result in unauthorized access (e.g.,

default/blank passwords), unauthorized elevation of privileges, or unauthorized remote code execution

ACRONYMS

A&A – Assessment and Authorization

ATO – Authority to Operate

CIO – Chief Information Officer

CVSS – Common Vulnerability Scoring System

ISO – Information System Owner

ISSO – Information System Security Officer

ITSO – Information Technology Security Officer

OS – Operating System

SAR – Security Assessment Report

REQUIREMENTS

- 1) Medium, High, and Critical vulnerabilities must be remediated. Informational and Low vulnerabilities do not require remediation, due to the minimal risk presented to NIST.
- 2) If applicable, an ISSO, in collaboration with an ISO and OU ITSO, must request to the NIST ITSO that a vulnerability be an accepted risk for an information system for which they are responsible. The NIST ITSO will review risk acceptance requests, and approve or deny based on the risk presented to NIST, including any compensating controls that may exist. Such acceptance is presented to Authorizing Officials for review and approval through a Security Assessment Report.

Operating System and Installed Applications

- 3) The NIST ITSO provides output from vulnerability scanning to OU Information Technology Security Officers (OU ITSO) and Information System Security Officers (ISSO) at least quarterly and for security assessment, with the following scope:
 - a) For internal assets, Critical vulnerabilities are reported. A general risk is accepted by the NIST CIO that not all active vulnerabilities and/or missing patches discovered, will be reported to ISSOs. However, ISSOs have access to all active vulnerabilities and/or missing patches discovered within the scanning tool.
 - b) For externally-accessible assets, Medium, High, and Critical vulnerabilities are reported.
- 4) The NIST ITSO tracks remediation of vulnerabilities through security assessments and Plans of Action & Milestones (POA&Ms), with the following scope:

- a) For internal assets, remediation of Critical vulnerabilities is tracked. A general risk is accepted by the NIST CIO that vulnerabilities and/or missing patches not reported and categorized other than Critical, may not be remediated. This acceptance is due to enterprise and system-level prioritization of resources, and in consideration of the volume of vulnerabilities.
- b) For externally-accessible assets and those being assessed for initial ATO, Medium, High, and Critical vulnerabilities are tracked.

Web-based Applications

- 5) Vulnerability scans of all internal and publicly available web applications are conducted at least annually, or when significant changes are made.
- 6) Medium, High, and Critical vulnerabilities of all internal and publicly available web applications are tracked through POA&Ms.

ROLES AND RESPONSIBILITIES

Authorizing Official

- Review security assessment reports
- Ensure risks are acceptable and POA&Ms are completed on schedule
- Approve/deny risk acceptance through a Security Assessment Report

NIST CIO

- Delegate risk acceptance review and approval to the NIST ITSO

NIST ITSO

- Approve/deny risk acceptance requests
- Approve vulnerability severity recommendations or elevate

OU IT Security Officer

- Oversee/facilitate remediation for OU information systems
- Review vulnerability reports
- Collaborate with ISO and ISSO as required; facilitating mitigation activities, requests for accepted risks, and status of POA&Ms, as necessary

Information System Owner

- Oversee ISSO in coordinating the remediation of identified vulnerabilities
- Ensure adequate resources to remediate identified vulnerabilities

Information System Security Officer

- Schedule and remediate identified vulnerabilities, and/or coordinate with system administration staff

- Collaborate with ISO and ITSO as required; prioritizing mitigation activities, submitting requests for accepted risks, and providing status of POA&Ms, as necessary

Security Control Assessor

- Administer vulnerability scanning
- Categorize vulnerabilities
- Recommend change to NIST ITSO in vulnerability severity
- Provide reports
- Manage risk request process
- Ensure mitigation actions through POA&M

System Administrator

- Mitigate identified vulnerabilities
- Complete POA&M action items
- Coordinate vulnerability remediation efforts with the ISSO

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

Appendix A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	3/12/2016	Carol Schmidt	New Draft
Rev .01	4/5/2016	Dan Cipra	Formatting changes

Privacy Data Loss Prevention

NIST S 6102.16

Issue Date: 8/5/2016

Effective Date: 8/5/2016

PURPOSE

This suborder directive defines the National Institute of Standards and Technology (NIST) efforts to enhance privacy protections and minimize the transmission of sensitive personally identifiable information (PII) through implementation of a Data Loss Prevention (DLP) tool on enterprise email services.

APPLICABILITY

This suborder applies to all NIST information system users that utilize NIST email services (e.g. incoming, outgoing, and internal to internal individual(s) and mail lists). This directive does not apply to encrypted email or web traffic.

REFERENCES

- [The Privacy Act of 1974](#)
- [Federal Information Security Modernization Act \(FISMA\) of 2002](#)
- [Office of Management and Budget \(OMB\) Memorandum M-06-16, *Protection of Sensitive Agency Information*](#)
- [OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*](#)
- [NIST Special Publication \(SP\) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*](#)
- [Department of Commerce \(DOC\) Memorandum on Departmental Privacy Standards for Commerce Data Loss Prevention \(DLP\) Security Tools, dated 04/15/2016](#)
- [DOC Privacy Data Loss Prevention \(DLP\) Working Group Recommendations, dated 12/17/2014](#)
- [DOC Memorandum on *Procedures on Notifying Management Officials of Individuals Who Fail to Safeguard Sensitive Personally Identifiable Information*, dated 08/03/2015](#)
- [O 6102.00 NIST Information Technology Program](#)

DEFINITIONS

Data Loss Prevention – minimizing the number of sensitive personally identifiable information email incidents through the use of automated tools (e.g. Microsoft Office 365)

that implement policies and processes to identify sensitive information stored throughout the NIST network, restrict access to that sensitive information, and monitor transmission of sensitive information in and out of the network boundary.

REQUIREMENTS

1. OISM shall employ Data Loss Prevention (DLP) on NIST enterprise email services.
2. OISM shall configure DLP with recommendations set forth in the *Department of Commerce Privacy Data Loss Prevention (DLP) Working Group Recommendations*, in so much as possible.
3. The DLP shall be configured to transmit a non-delivery report/receipt (NDR) email message to a sender when the DLP detects PII within the subject line, body, or attachment of a message.
4. Upon receipt of a NDR email message, the sender shall review the email for offending personally identifiable information (PII), recompose/alter the email to remove, and retransmit.
5. If the sender cannot locate offending PII and believes the DLP tool detected a false positive (e.g. DLP blocked sending, but email doesn't contain PII), the user shall contact the IT Assistance Center (iTAC). Support shall be limited to assisting the NIST end user in applying encryption technology to the email.
6. The following DLP metrics/reporting shall be compiled by OISM:
 - Total DLP events (e.g., total number of emails that were blocked with a non-delivery receipt (NDR) message). Inbound messages determined to be sent from another agency shall result in notification to the agency's incident response team.;
 - Total DLP false positives (e.g., those reported by users through iTAC);
 - Total DLP users which had multiple (e.g., more than one) blocked emails;
 - Total DLP events which, if not blocked, impose a significant risk to NIST (e.g., an email and/or attachment containing multiple Social Security Numbers). These events shall be considered a reportable incident even though the transmission was blocked.
7. Waiver requests or exceptions to DLP security control requirements shall follow procedures located at: https://inet.nist.gov/oism/howdoi/iss_waivers.cfm

ROLES AND RESPONSIBILITIES

Office of Information Systems Management

- Administer the DLP tool (e.g., configure filter)
- Provide Tier I and Tier II support to internal users
- Provide NIST metrics and reporting on DLP
- Notify Information System Owner (as applicable) and Supervisor of users which had multiple blocked emails

Information Systems Users

- Review and recompose/alter an offending email, and retransmit
- Contact iTAC for encryption support

Information Systems Owners

- Ensure email servers within their purview apply DLP

Supervisors

- Take appropriate action for users which had multiple (e.g., more than one) blocked emails

DIRECTIVE OWNER

18 Office of Information Systems Management

APPENDICES

A. Revision History

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial		Islelly Castillo	draft
Rev. .01	8/15/2016	Carol Schmidt	Updated links, added reference

Web-Based Voice/Video Conferencing Services and/or Software Product Use

NIST S 6102.18

Issue Date: 9/25/2014

Effective Date: 8/16/2012

PURPOSE

The purpose of this directive is to define requirements for the secure use of web-based conference services and/or software in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users of web-based conferencing services/software on NIST information systems.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.”](#) Access Control (AC) and System and Communication Protection (SC) families.

REQUIREMENTS

1. Only public or non-sensitive (i.e., low confidentiality) sessions are permitted unless using a service that includes encryption using a FIPS 140-2 validated cryptographic module and where a full security assessment has been performed by the Office of Information Systems Management (OISM).
2. Web-based conferencing services/software must be able to function as intended without having to implement or change NIST firewall policies or NIST network configurations.
3. The installation and use of web-based conferencing services/software for hosting must be documented in relevant System Security Plans.

DIRECTIVE OWNER

18 – [Office of Information Systems Management](#)

Information System Contingency Plan Testing

NIST S 6102.25

Issue Date: 8/19/2015

Effective Date: 08/29/2011

PURPOSE

The purpose of this directive is to define requirements for Information System Contingency Plan in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system resources used in the conduct of NIST business.

REFERENCES

- [NIST information security directives](#);
- This directive is supplemental to a suite of security controls consisting of:
 - [Commerce Information Technology Requirement \(CITR-015\) “Contingency Plan Testing and Exercise Activities”](#);
 - [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
 - [NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.”](#) Contingency Planning (CP) family.

REQUIREMENTS

1. Contingency plan testing must be conducted based on the information system’s FIPS-199 rating for availability.
2. Contingency plans (including tests) must be part of a system security plan using templates and testing requirements provided by OISM.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

- A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	8/18/2015	Deb Dubeau	

Use of Electronic Signatures

NIST S 6102.28

Issue Date: 8/11/2015

Effective Date: 8/11/2015

PURPOSE

This directive defines requirements for implementing the use of electronic signatures in support of NIST programs.

BACKGROUND

Electronic signatures must be functionally equivalent to the signature applied to a paper record. The goal is to specify criteria which, once met by an electronic signature, enable the signature to have the same level of legal recognition as a corresponding handwritten signature without imposing more stringent standards of security. To be functionally equivalent to a handwritten signature, the E-Transaction laws require that the electronic form of signature must be made part of the record being signed (i.e., being attached to or logically associated with the record being signed).

APPLICABILITY

This directive applies to all electronic records where a legally binding electronic signature is required.

REFERENCES

- [Access and Use of Information Technology Resources O 6103.00;](#)
- [Access and Use of Electronic Signatures N 6103.22;](#)
- This directive is supplemental to a suite of security controls consisting of:
 - [Commerce Information Technology Requirements;](#)
 - [DOC Information Technology Security Program Policy \(ITSP\);](#)
 - [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations;"](#)
 - [National Archives and Records Administration \(NARA\) Transmittal 23 part GRS 3.2 items 060-062;](#)
- [Use of Electronic Signatures in Federal Organization Transactions;](#)

- [Electronic Signatures in Global and National Commerce Act, PL 106-229](#);
- [OMB Memorandum 00-10, Procedures and Guidance on Implementing the Government Paperwork Reduction Act](#); and
- E-Transaction Laws:
 - *Government [Paperwork Elimination Act \(GPEA\)](#)*;
 - [Electronic Signatures in Global and National Commerce Act \(E-SIGN\)](#); and
 - [Uniform Electronic Transactions Act \(UETA\)](#).

REQUIREMENTS

1. The signing process must satisfy the following requirements for a legally binding electronic signature:
 - a. A person (i.e., the signer) must use an acceptable electronic form of signature.
 - b. The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record (e.g., to indicate a person's approval of the information contained in the electronic record).
 - c. The electronic form of signature must be attached to or associated with the electronic record being signed.
 - d. There must be a means to identify and authenticate a particular person as the signer.
 - e. Cached credentials must not be used when applying a signature (i.e., user must be prompted to authenticate each time a signature is applied).
 - f. There must be a means to preserve the integrity of the signed record (i.e., ensure that the signatures become invalid if changes are made after signatures are applied).
 - g. The signing process must be supported by a workflow, to include:
 - i. Routing and tracking
 - ii. Record archival
 - iii. Reporting (e.g., record retrieval)
 - h. The following data elements must be appended to, or associated with, the signature data provided privacy considerations have been taken into account:
 - i. Identity of the signer or a link to the source of identifying information (e.g., a validated userid, a digital certificate on a PIV card, a biometric database, etc.).
 - ii. Date and time of the signature.
 - iii. Method (e.g., typed name, scanned image of a handwritten signature, or the clicking of an "accept" button) used to sign the record.
 - iv. An indication of the reason for signing (i.e., approval, acknowledgement, etc.).
2. Where digital signature is required by the signing process, it must be based on certificates issued from an approved, trusted, and legitimate certificate authority (CA).

3. Signatures must be based on individual user credentials and not based on group or functional credentials.

RESPONSIBILITIES

Business and/or Process Owner

- Responsible for understanding the business requirements under their purview and determining legal, security, or other requirements which would govern the use and selection of a particular type of electronic signature process.
- Responsible for authorizing the use of electronic signatures on records in their area of responsibility.
- Responsible for defining the signing process which fulfills the legal and business requirements associated with signing an electronic record.
- Responsible for communicating and documenting approved signing process, electronic or otherwise, associated with signing a record.
- Responsible for management of the signed electronic record in accordance with NARA Records Schedules.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change

Access and Use of Information Technology Resources

NIST O 6103.00

Issue Date: 10/17/2016

Effective Date: 10/17/2016

PURPOSE

The purpose of this directive is to define requirements for access and use of NIST information and technology (IT) resources based on requirements as stated in the Commerce Information Technology Requirements (CITR-022) Access and Use Policy.

APPLICABILITY

- This directive applies to all NIST employees, contractors and other associates (to include non-employee students, post-docs, guest researchers, etc.), regardless of whether information technology (IT) accounts are assigned, or credentials issued; and
- All access to DOC information and IT resources, regardless of the device, network, infrastructure, or location (e.g., remote connection to a DOC network). Network access to information and services may include wired, wireless, or remote, and may include domestic or foreign destinations. Regardless of the infrastructure used to access DOC information and IT resources, access and use rules defined herein apply.

LEGAL AUTHORITIES AND REFERENCES

- [The Privacy Act of 1974](#), 5 U.S.C. § 552a;
- [M-04-26, Memorandum for the Chief Information Officers on Personal Use Policies and “File Sharing” Technology](#), Office of Management and Budget, 2004;
- [M-07-16, Memorandum for the Heads of Executive Departments and Agencies on Safeguarding Against and Responding to the Breach of Personally Identifiable Information](#), Office of Management and Budget, 2007;
- [Standards of Ethical Conduct for Employees of the Executive Branch](#); and
- [Department Administrative Order 202-751: Discipline](#), United States Department of Commerce, 1980;
- [Commerce Information Technology Requirement \(CITR-022\) Access and Use](#);
- [Privacy Policy, United States Department of Commerce](#), 2008;
- [DOC Information Technology Security Program Policy \(ITSPP\)](#);
- [Ethics Rules](#), United States Department of Commerce Office of Assistant General Counsel for Administration Ethics Law and Programs Division, 2013;

- [Ethics Clearance for Combined Federal Campaign Fund Raising Events, October, 2013.](#)
- NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Access Control (AC) family;
- [P 6100.00 Information Systems Management and Use Policy](#);

BACKGROUND

As stated in the Commerce Information Technology Requirement (CITR-022), the DOC promotes job creation, economic growth, sustainable development, and improved standards of living for all Americans by working in partnership with businesses, universities, communities, and our nation’s workers. Information is at the core of this mission, and thus other than its personnel and customers, DOC considers information as one of its most valuable assets. Technology has enabled DOC to create efficiencies in its work and has become an imperative tool in the operation and conduct of work and to the services provided to its customers.

Given that information is an asset, DOC strives to protect the confidentiality, integrity, and availability of its information and technological resources, and thus imposes a baseline security categorization on all its information. This means that all non-public DOC information requires at least minimum security controls (i.e., low) to protect it. Some of this information, such as personally identifiable information (PII), financial, or other types of information which require protection from unauthorized disclosure, require more stringent security controls (e.g., use of encryption). This more sensitive information must be protected using at least a moderate level of security. While automated means are in place to enhance security, each DOC user of information and associated technology has a duty to protect information at its defined level.

This directive replaces the NIST Access and Use Policy for IT Resources directive (O601), dated 2003.

REQUIREMENTS

Requirements defined herein are taken directly from the CITR-022, Access and Use Policy. Supplemental, issue-specific NIST rules are contained in a series of Notices titled, [Access and Use](#). NIST information system users must report IT incidents by contacting the Information Technology Assistance Center (iTAC) (301-975-5375 or 303-497-5375 or itac@nist.gov).

1. DOC information and IT resources may be used in the conduct of mission-related work, in the administration and management of DOC programs, and in the dissemination of the results of DOC work. The general criteria used in deciding acceptable access and use are based on general ethical principles of conduct, as well as government policies and statutory requirements.
2. DOC permits limited personal use of its information and IT resources, including telecommunication services, provided that such access complies with the requirements defined herein, does not interfere with DOC work and individual duties, and does not

increase costs to the government or to the DOC. Such limited personal access and use is a privilege, not a right, and is by no means universal among Federal agencies.

3. Employees and associates are expected to conduct themselves professionally in the workplace and refrain from using information and IT resources, including telecommunications services, for activities that are not authorized under existing laws, regulations, or DOC policies. Unacceptable and prohibited uses of DOC IT resources, systems, and networks include, but are not limited to:
 - a. Use of electronic devices, systems or services for the following:
 - i. Unauthorized physical or wireless connection of unapproved IT devices to internal DOC IT resources (e.g., the connection of personal smart phones or cameras for purposes of charging the battery source or accessing information, or the connection and use of personal flash drives or personal removable hard drives);
 - ii. Unauthorized use of non-DOC contracted cloud services to store DOC information;
 - iii. Electronic transmission of unencrypted sensitive information (e.g., PII) across the Internet;
 - iv. Unauthorized remote access services or mechanisms designed to bypass authorized remote access services;
 - v. Use of personally owned mobile devices and media to store sensitive DOC information;
 - vi. Unauthorized forwarding or synchronization of email or other internal DOC information or records to personally owned devices or resources;
 - vii. Installation of software on DOC IT resources that is not work-related or that has been explicitly prohibited;
 - viii. Access to any network or system for which the person has not been authorized, or in a manner that knowingly violates DOC policies;
 - ix. Unauthorized use of a system for which the user has authorized access (e.g., accessing information not needed to conduct one's official duties, or unauthorized use of privileged commands). For example, no user may access the root account on a Unix system or attempt to access the most privileged accounts on the system unless he or she is authorized and has a reason to do so; and
 - x. Sharing individual authentication credentials (e.g., smartcard, token, authenticator, PINs, passwords, etc.) with users for whom access to those credentials is not explicitly authorized.
 - b. Use of DOC IT resources to conduct or participate in unethical or illegal activities:
 - i. The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;

- ii. The intentional creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal or otherwise prohibited activities;
 - iii. The intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any DOC or OU-defined controlled information including, but not limited to, software and information that includes privacy information, copyrighted, trademarked, or otherwise protected intellectual property (beyond fair use), proprietary data, or export controlled software or data;
 - iv. Activities which are inappropriate or offensive to fellow employees, associates, or the public. Such activities include: harassment, hate speech, or material that discriminates against others on the basis of race, creed, religion, color, age, gender, disability, national origin, or sexual orientation;
 - v. The use of government IT resources for unauthorized commercial purposes, “for-profit” activities for an individual or company, or other outside employment or business activity (such as consulting for pay, sales or administration of business transactions, sale of goods or services); and
 - vi. Engaging in any unauthorized fundraising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
 - c. Inappropriate use of DOC IT resources:
 - i. Unauthorized dissemination of non-public DOC information to external parties or entities that are not authorized to view them, such as newsgroups, bulletin boards, or other public forums;
 - ii. Use or creation of personal or otherwise unauthorized list servers;
 - iii. Establishing personal, commercial, and/or non-profit organizational web pages on government owned or operated information systems;
 - iv. Unauthorized creation, copying, transmission, or retransmission of chain letters, unauthorized newsletters, or other unauthorized mass mailings regardless of the subject matter.
 - d. Exceeding information transfer thresholds for DOC IT resources, which could cause congestion, delay, or disruption of service to the legitimate activities of anyone using DOC IT resources. For example, excessive (in proportion to resources) media streaming, or sending or downloading of excessively large file attachments can degrade the performance of the entire network.
4. Official DOC work and digital communications (e.g., email) must be carried out using authorized DOC IT accounts. Official DOC communications are defined as any transfer of signs, writing, images, data, or intelligence for the purpose of supporting a DOC mission or objective. Use of personal accounts for official work or communications is prohibited. There may be circumstances that warrant deviations (e.g., where there is an

imminent risk to life or property, an official communication related to an emergency may be made through the use of personal email).

5. Records and information must be retained if:
 - a. Regulation or statute requires their retention;
 - b. Management determines they are likely to be needed for investigation or prosecution of unauthorized, illegal, or abusive acts;
 - c. Management determines they are likely to be needed in the future.
6. Electronic records are required to be maintained in accordance with a National Archives and Records Administration (NARA) approved record schedule, and appropriate backups maintained and tested.
7. Employees and associates shall not destroy or dispose of the DOC's records or information without advance management approval. The use of social media may create Federal records that must be captured and managed in compliance with Federal records management laws, regulations, and policies.
8. Routine continuous monitoring of networks and IT systems is conducted to identify and respond to performance-degrading events such as equipment failures, capacity issues, security threats, and security breaches. Therefore, all employees and associates using DOC systems should be aware that information transmitted by or stored on systems within DOC's purview is not private.
9. While in official duty status, employees may not use technology to secretly overhear, transmit, or record communications. In lieu of a reporter or secretary taking verbatim transcriptions or notes of conferences or meetings, conventional conference equipment may be utilized, provided that advance notice is given to, and approval obtained from the participants in the conference or meeting.
10. Personal photography is generally authorized without prior permission, however, photography of sensitive areas, equipment, or documentation is prohibited. Further, DOC policy requires mutual consent to photograph or record guest speakers, officials or activities.
11. All DOC employees and associates must promptly report incidents involving information and information technology resources. Incidents may include suspected or confirmed presence of malware, policy violations, misuse, loss or breach of PII, loss or theft of a smartcard, smartphone, laptop, tablet, etc. Further, employees and associates may not impede actions taken to conduct a forensic evaluation and/or sanitize information technology resources. DOC management has an even greater responsibility to report and remediate incidents as soon as they are observed and/or reported to them so as to reduce the risk and liability to the DOC.
12. Unacceptable access and/or use of DOC information and information technology resources by employees may subject the employee(s) to discipline in accordance with existing DOC policy, including the penalties provided in Department Administrative Order (DAO) 202-751, Discipline (see reference in Section 7).

13. Unacceptable access and/or use by contractors or other associates will result in notifications to the host organization management and may result in similar penalties and possible termination of agreement to work with DOC.
14. Employees, contractors or other associates engaging in unacceptable access and/or use shall also be subject to having all IT accounts and/or other credentials indefinitely suspended at the discretion of DOC and/or OU management and the Departmental and/or OU Chief Information Officer.

RESPONSIBILITIES

Office of Information Systems Management

- Enforces formal acknowledgment of Access and Use rules.

NIST Supervisors

- Ensures compliance with Access and Use rules.

Information System Users

- Reads, understands, acknowledges, and adheres to this Order and supplemental Access and Use Notices.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Version		Deb Dubeau	Draft
Rev. .01	8/5/14	Dan Cipra	Formatting changes only
Rev. .02	6/21/2016	Islelly Castillo	Updated with new verbiage and added FAQ
Rev. .03	10/5/2016	Dan Cipra	Incorporated DRB updates

Access and Use of Web-Based Voice/Video Conferencing Services and/or Software Product Use

NIST N 6103.06

Issue Date: 8/5/2014

Effective Date: 8/16/2012

PURPOSE

The purpose of this directive is to define requirements for the secure use of web-based conference services and/or software in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Interim Technical Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."](#) Access Control (AC) and System and Communication Protection (SC) families.

REQUIREMENTS

If participating in or hosting web-based conference sessions the user must:

1. Use NIST or NIST Organizational Unit (OU) supported web-based conferencing services/software. If it is not possible to use a NIST or NIST OU supported service:
 - Coordinate use of an alternative web-based conferencing services/software with OU Information Technology Security Officer (ITSO) prior to use.
 - Use web-based conferencing services/software that does not include peer2peer (P2P) technology. Examples of prohibited technology includes BitTorrent, Napster, KaZaA, etc.
2. Use web-based conferencing services/software for official business only.
3. Use only public or non-sensitive (i.e., low confidentiality) sessions.

If hosting a web-based conference session the user must:

1. Monitor the entire active session. The host must be fully cognizant of the sensitivity (confidentiality) of the information being shared, the protection provided by the conference service (i.e., tool) and venue (i.e., physical location).
2. Restrict remote control access during a session unless it is absolutely necessary and approved according to any relevant OU policies. Remote control access includes remote control of the Operating System (OS) functionality, remote control of applications, and remote access to NIST systems and services. During a session that includes remote control, the session must be actively and carefully monitored by the User/Host to ensure access is appropriate and necessary.
3. Challenge and/or shut down the session if unauthorized activities occur (e.g., activities prohibited by other NIST directives including access to internal NIST sites and systems not relevant to the hosted session) or access to sensitive information becomes likely. Report any unauthorized activities or access to the appropriate OU ITSO and the Information Technology Assistance Center (iTAC x5375).
4. Prohibit use of web-based conferencing services and other Internet remote access services (e.g., gotomypc or logmein remote access) for access to NIST systems and networks.

DIRECTIVE OWNER

18 – Office of Information Systems Management

APPENDICES

A – Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	1/30/2014	Deb Dubeau	Converted the PR 641 to a Notice
Ver .01	7/11/14	Deb Dubeau	Modified based on DRB Comments

Access and Use of BitTorrent Peer-to-Peer File Sharing

NIST N 6103.07

Issue Date: 8/5/2014

Effective Date: 04/09/2010

PURPOSE

The purpose of this directive is to define requirements for the use of BitTorrent Peer-to-Peer (P2P) file sharing technology in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Interim Technical Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) System and Services Acquisition (SA) family;
- Office of Management and Budget (OMB) Memorandum [M-04-26](#), Personal Use Policies and File Sharing Technology.

REQUIREMENTS

1. The use of BitTorrent file sharing technology is approved for use at NIST only under the following conditions:
 - BitTorrent installed on NIST-owned computers and/or any devices connected to NIST networks must only be enabled and used for official business, and when such use considers the sensitivity of the data being exchanged.
 - BitTorrent may only be used when there is no other practical approved application or mechanism to transmit required files.
 - BitTorrent must be disabled when not in use.
 - As technically feasible, BitTorrent must be configured to prohibit uploads from NIST computers to external computers.
2. BitTorrent usage, including the work-related purpose and configuration, must be documented and approved in the relevant information system security plan.

DIRECTIVE OWNER

18 - Office of Information System Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	4/24/13	Deb Dubeau	New Notice replacing O 603.
Ver .01	8/28/13	Dan Cipra	Updated formatting.

Access and Use, Personal Identity Verification Card Authentication to Information Systems

NIST N 6103.09

Issue Date: 11/26/2013

Effective Date: 11/26/2013

PURPOSE

The purpose of this directive is to define the requirements for using Personal Identity Verification (PIV) cards for authentication to information systems.

APPLICABILITY *(When the overarching policy regarding PIV cards is published, this Applicability section will be revised to indicate that this directive applies to all NIST information system users who have PIV cards.)*

This directive applies to all NIST information system users that are eligible for a PIV card.

- To be a NIST information system user, the individual shall have signed a NIST IT Access and Use agreement certifying that they will adhere to NIST IT policies.
- An information system user is eligible for a PIV card if they meet the following requirements:
 - a. Must have a Social Security Number;
 - b. Must have an expected length of federal service greater than 179 days or an expected agreement term greater than 179 days; and
 - c. Are expected to be physically onsite at NIST more than 179 cumulative days.

REFERENCE

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Interim Technical Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#);
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"](#), Identification and Authorization (IA) family;
- [FIPS 201-1, "Personal Identity Verification \(PIV\) of Federal Employees and Contractors"](#);
- [Homeland Security Presidential Directive \(HSPD\) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors"](#);
- [OMB Memorandum 05-24, "Implementation of HSPD 12"](#);

- [OMB Memorandum 11-11, “Continued Implementation of HSPD 12”; and](#)
- [Federal Chief Information Officers \(CIO\) Council and Federal Enterprise Architecture \(EA\), “Federal Identity, Credential and Access Management \(FICAM\) Roadmap and Implementation Guidance v1.0”.](#)

REQUIREMENTS

1. Information system users shall obtain and maintain a current PIV card.
2. Information system users shall use their assigned PIV card to authenticate to PIV enabled information systems. Alternative authentication methods may be used, as available, when users are unable to use their PIV card to authenticate.
3. Information system users shall not share their assigned PIV card or associated PIN, and shall protect each appropriately.
4. Information system users shall report lost or stolen PIV cards immediately.

DIRECTIVE OWNER

181 - [Office of Information Systems Management](#)

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	8/14/2013	Deb Dubeau	First Draft
Rev. .01	10/25/2013	Melissa Lieberman	OCC comments
Rev. .02	11/15/2013	Deb Dubeau	DRB Comments
Rev. .03	11/19/2013	Dan Cipra	DRB Meeting edits
Rev. 04	2/2/2016	Dan Cipra	Updated new directive number (N 654.01)

Access and Use of IT While on Foreign Travel

NIST N6103.10

Issue Date: 5/4/2015

Effective Date: 5/4/2015

PURPOSE

The purpose of this directive is to define requirements for access and use of IT (e.g., laptops, tablets, smartphones, removable media storage devices, etc.) by travelers while in foreign destinations supporting NIST programs.

APPLICABILITY

This directive applies to all NIST information system users and resources used in the conduct of NIST business from foreign destinations, regardless of whether travel is official or personal.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [Access and Use of Information Technology Resources O6103.00](#);
- [Commerce Information Technology Requirement \(CITR\)-020](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."](#)

REQUIREMENTS

1. Users must only use IT which is part of an approved OISM Loaner Laptop for Foreign Travel Pool, Foreign Travel Mobile Device Pool, or Organizational Unit (OU) Loaner Pool which adheres to the requirements set forth in [CITR-020](#) Safeguarding Information While on Foreign Travel.
2. Users must ensure physical security of NIST mobile devices and removable media.
3. Users must only use IT which is encrypted using FIPS 140-2 validated encryption.
4. Users must not attempt to modify the configuration of the device loaned to them. However, users may install additional business-related software, as necessary.
 - Email client software must not be installed on laptops.
5. Users must fully power down devices when not in use and shall remove the battery, if possible, while attending meetings in which sensitive or proprietary information is discussed.

6. Users must not connect non-NIST portable media (e.g., personally owned, conference issued flash drives, etc.) to a NIST computer.
7. Users must not connect non-NIST owned devices to the internal NIST network from outside the U.S.
8. Users must not store NIST information in personally owned cloud storage services.
9. Users must take additional precautions when accessing or taking sensitive data:
 - take only information that is necessary; and
 - notify and obtain authorization from management when taking sensitive information.
10. Upon return, users must not connect IT used while on foreign travel to the internal NIST network.
11. Loaner devices must be returned to the Foreign Travel Loaner Pool for scanning and sanitization.
12. Waiver requests for these requirements must follow procedures located at:
https://inet.nist.gov/oism/howdoi/iss_waivers.cfm

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	3/16/2015	Deb Dubeau	
Rev. .01	4/28/2015	Dan Cipra	Formating updates only

Access and Use of Automatic Email Forwarding

NIST N 6103.12

Issue Date: 4/1/2015

Effective Date: 01/28/2009

PURPOSE

The purpose of this directive is to define requirements for the automatic forwarding of NIST email. Specifically, this applies to individual email accounts.

APPLICABILITY

This directive applies to all NIST information system users and information system resources used in the conduct of NIST business.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [Access and Use of Information Technology Resources O 6103.00](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"](#).

REQUIREMENTS

1. Automatic forwarding of NIST email must only be permitted with an approved waiver from an Operating Unit (OU) Director.
 - Waiver requests for these requirements must follow instructions located at: https://inet.nist.gov/oism/howdoi/iss_waivers.cfm
2. Waivers for automatic email forwarding must not be approved for:
 - Email accounts hosted outside the United States;
 - Personal email accounts (e.g., @gmail.com, @hotmail.com, etc.)
 - Corporate and commercial email accounts (e.g., @domain.com, @domain.biz, etc.); and
 - Individuals no longer associated with NIST (i.e., former NIST employees and associates).
3. Waiver approvals must be based on a supporting business justification (e.g., forwarding email to NIST employees or associates who spend a substantial amount of time at an

organization which has a formal relationship with NIST). Examples of acceptable email accounts include:

- Email accounts associated with the United States Federal Government (e.g., @doc.gov, @usmc.mil); and
 - Email accounts associated with an organization (e.g., @domain.org, @domain.net, or @domain.us) or academic institution (e.g., @domain.edu) that has established a formal relationship with NIST.
4. NIST email accounts with an approved waiver must be configured to store email messages on a NIST-sponsored email server, and automatically forward a copy to the approved email account.
 5. NIST email accounts without an approved waiver must not be configured to automatically forward.
 6. OISM will enforce these requirements, and terminate automatic forwarding where an approved waiver does not exist.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
	2/23/2015	Deb Dubeau	Initial draft
Rev. .01			

Access and Use of Dropbox

NIST N 6103.13

Issue Date: 12/23/2014

Effective Date: 09/21/2011

PURPOSE

The purpose of this directive is to define requirements prohibiting the access and use of Dropbox Internet file hosting service in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users, all NIST information system resources, including NIST desktops, laptops, mobile devices, servers, and other computers, and all other information system resources connected to NIST networks. This directive does not apply to NIST networks specifically authorized for personally owned devices (e.g., NIST-Visitor wireless network).

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [O 6103.00 Access and Use of Information Technology Resources](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Access Control (AC) family.

REQUIREMENTS

1. Information system users are prohibited from installing and using Dropbox software.
2. Dropbox software must not be used on personally owned equipment while connected remotely to NIST networks.
3. Computers found to have Dropbox software installed will be removed from the NIST network immediately, and will remain off the network until OISM staff or an OU IT Security Officer has verified and documented that the software has been uninstalled.

DEFINITIONS

Dropbox – An Internet file hosting service that enables the storage and exchange of files.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES**A. Revision History**

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	10/22/2014	Deb Dubeau	Ready for DRB
Rev 1	11/19/2014	Dan Cipra	Formatting changes only
Rev 2	12/19/14	Dan Cipra	Incorporated all of the DRB comments.

Access and Use of Remote Connection to NIST

NIST N 6103.14

Issue Date: 5/4/2015

Effective Date: 10/15/2008

PURPOSE

The purpose of this directive is to define requirements for remote access and use of NIST information and technological resources in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users and all NIST information system resources used in the conduct of NIST business. This includes remote access to internal NIST networks, however, this does not include NIST networks specifically authorized for personally owned devices.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [Access and Use of Information Technology Resources O 6103.00](#);
- [Commerce Information Technology Requirement CITR-008](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."](#)

REQUIREMENTS

1. Only NIST authorized information system users are permitted to use a remote connection to internal NIST networks and systems. Family members, friends, or any other unauthorized user must not be permitted access to the device while it is remotely connected to internal NIST networks and systems.
2. NIST information system users must ensure the physical security of devices used for remote access (e.g., do not leave unattended in public areas).
3. When non-government owned (e.g., personally owned, etc.) computers are used for remote access they must be authorized (e.g., key file) and the following secure configuration/practices must be observed:
 - a. Use personal firewalls.
 - b. Use anti-virus protection.
 - c. Uninstall or disable prohibited software while connected remotely to NIST internal networks. Prohibited software includes, but is not limited to, Peer-to-

Peer (P2P) file sharing (e.g., BitTorrent eDonkey, FlashGet, BearShare, etc.), Skype, software integrated with Skype (e.g., MySpace Instant Messenger), and Hamachi virtual private network software.

- d. Configure applications to not store NIST passwords.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	3/16/2015	Deb Dubeau	
Rev. .01	4/28/2015	Dan Cipra	Format changes only

Access and Use of Skype

NIST N6103.15

Issue Date: 12/23/2014

Effective Date: 03/16/2006

PURPOSE

The purpose of this directive is to define requirements prohibiting the use of Skype Voice over Internet Protocol (VoIP) software in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users, all NIST information system resources, including NIST desktops, laptops, mobile devices, servers, and other computers, and all other information system resources connected to NIST networks. This directive does not apply to NIST networks specifically authorized for personally owned devices (e.g., NIST-Visitor wireless network).

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [O 6103.00 Access and Use of Information Technology Resources](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Configuration Management (CM) family.

REQUIREMENTS

1. Information system users are prohibited from installing and using Skype software.
2. Skype software must not be used on personally owned equipment while connected remotely to NIST networks.
3. Computers found to have Skype software installed, will be removed from the NIST network immediately, and will remain off the network until OISM staff or an OU IT Security Officer has verified and documented that the software has been uninstalled.

DEFINITIONS

Skype – An Internet service and client software which enables voice, video, and instant messaging communication with peers by voice, video, and instant messaging.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	10/22/2014	Deb Dubeau	Ready for DRB
Rev. .01	11/19/2014	Dan Cipra	Formatting changes only

Access and Use of Microsoft Windows 8

NIST N 6103.20

Issue Date: 8/5/2014

Effective Date: 08/16/2012

PURPOSE

The purpose of this directive is to define requirements for the use of the Microsoft Windows 8 operating system in support of NIST programs.

APPLICABILITY

This directive applies to all NIST information system users.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- O6103 Access and Use of Information Technology Resources;
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53](#), “Security and Privacy Controls for Federal Information Systems and Organizations.”

REQUIREMENTS

1. The use of the Windows 8 operating system on any device connected to a NIST network is prohibited. This prohibition includes operation of virtual instances of Windows 8.
2. The Windows 8 operating system may be installed and used on NIST computers not connected to any NIST network. It should be noted that OISM cannot guarantee any form of support for Windows 8.
3. Waiver requests for these requirements must follow procedures located at: https://inet.nist.gov/oism/howdoi/iss_waivers.cfm
4. This prohibition does not apply to NIST staff remotely accessing (e.g., from home) the NIST network using computers running Windows 8. However, it should be noted that OISM cannot guarantee compatibility with the NIST remote access services (i.e., SSL Remote Access), and OISM will not be able to provide support for anyone that is trying to remotely access the NIST network from a computer using Windows 8.

DIRECTIVE OWNER

18 – Office of Information Systems Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	1/8/2014	Deb Dubeau	Initial draft revision
Updates	2/6/2014	Dan Cipra	Formatting changes only. Responsibilities section question answered.

Access and Use of Microsoft Windows Vista

NIST N 6103.21

Issue Date: 11/25/2013

Effective Date: 07/22/2009

PURPOSE

The purpose of this directive is to define requirements for using the Windows Vista operating system.

APPLICABILITY

This directive applies to the use of the Microsoft Vista operating system on computers or other IT enabled equipment connected to the internal NIST network.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- NIST information security directives;
- Commerce Interim Technical Requirements;
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53](#), “Security and Privacy Controls for Federal Information Systems and Organizations”, Configuration Management (CM) family.

REQUIREMENTS

Computers or other IT-enabled devices using the Microsoft Vista operating system shall:

1. not be connected to internal NIST networks;
2. be configured to meet all relevant security requirements, including patch management as required by CITS-016 and those in the [Secure Configurations](#) directive;
3. have anti-virus software installed and configured with up-to-date anti-virus definitions and auto-protect (or equivalent) enabled;
4. be documented under an accredited IT security plan belonging to the Organizational Unit (OU) managed computer; and
5. be documented in the Automated NIST Tracking System (ANTS) located online at <https://ants.nist.gov>.

6. Waiver requests are permitted, but shall follow submission [procedures](#).

DIRECTIVE OWNER

18 – Office of Information Systems Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	1/8/2014	Deb Dubeau	Initial draft revision
Updates	2/6/2014	Dan Cipra	Formatting changes only. Responsibilities section question answered.

Access and Use of Electronic Signatures

NIST N 6103.22

Issue Date: 7/28/2015

Effective Date: 7/28/2015

PURPOSE

This directive defines requirements for the use of electronic signatures in support of NIST business.

APPLICABILITY

This directive applies to all NIST information system users and NIST processes when a legally binding electronic signature is required.

REFERENCES

- [Access and Use of Information Technology Resources O 6103.00;](#)
- Use of Electronic Signatures S 6102.28;
- This directive is supplemental to a suite of security controls consisting of:
 - [Commerce Information Technology Requirements;](#)
 - [DOC Information Technology Security Program Policy \(ITSP\);](#)
 - [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations;"](#)
 - [National Archives and Records Administration \(NARA\) Transmittal 23 part GRS 3.2 items 060-062;](#)
- [Use of Electronic Signatures in Federal Organization Transactions;](#)
- [Electronic Signatures in Global and National Commerce Act, PL 106-229;](#)
- [OMB Memorandum 00-10, Procedures and Guidance on Implementing the Government Paperwork Reduction Act;](#) and
- E-Transaction Laws:
 - Government [Paperwork](#) Elimination Act (GPEA);
 - [Electronic Signatures in Global and National Commerce Act \(E-SIGN\);](#) and
 - [Uniform Electronic Transactions Act \(UETA\).](#)

DEFINITIONS

The definitions supplied below provide information on the topic of electronic signature when used in this, or other NIST directives on this topic.

Business and/or Process Owner – Manager who has the authority to make changes to a business process and the subsequent results.

Electronic Signature – The electronic equivalent of a handwritten signature indicating intent to agree to or approve the contents of a document. It is a generic, technology-neutral term that refers to the various methods by which one can “sign” an electronic record. Electronic forms of signature may be a typed name, a scanned image of a handwritten signature, or the clicking of an “accept” button coupled with user authentication. Properly executed, an electronic signature may be legally binding, but lack the measures for preventing forgery and information tampering provided by digital signature technology.

Digital Signature – The term used to describe the small segment of data produced when a specific mathematical process (involving a hash algorithm and public key cryptography) is applied to an electronic record. Also known as an advanced, standard, or secure electronic signature, digital signatures are based on Public Key Infrastructure (PKI) technology and are commonly used to verify the integrity and authenticity of software, email, or financial transactions, and other scenarios in which it is important to detect forgery or tampering. Where a digital signature is intended to be used as a legally binding signature, it is simply considered to be one form of an electronic signature.

Electronic Record – A document, form, or other record created, generated, sent, communicated, received, or stored by electronic means.

Legally Binding Electronic Signature – Where an electronic signature is required or otherwise deemed desirable, it is critical that the electronic signature and the associated signing process satisfy all of the applicable legal requirements.

Signing Process – The set of actions, steps, and elements used to create a legally binding electronic signature including application of an electronic form of signature to an electronic record and one or more processes or security procedures to address the other signature requirements of a legally binding signature, including identifying and authenticating the signer and ensuring integrity of the electronic record.

Workflow – The set of discrete steps in a business process, coupled with the transition between steps (e.g., including reverse transitions).

REQUIREMENTS

1. An electronic signature may be used to sign electronic records as specified by the Business and/or Process Owner.
2. Only signing processes approved by the Business and/or Process Owner may be used for electronic signatures.

RESPONSIBILITIES

Business and/or Process Owner

- Understands the business requirements under their purview and determines legal, security, or other requirements which would govern the use and selection of a particular type of electronic signature process.
- Defines the signing process which fulfills the legal and business requirements associated with signing an electronic record.
- Communicates and documents approved signing processes, electronic or otherwise, associated with signing a record.
- Authorizes the use of electronic signatures on records in their area of responsibility.
- Manages the signed electronic record in accordance with NARA approved Records Schedules.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	5/1/2015	Deb Dubeau	
Rev. .01	5/7/2015	Dan Cipra	Formatting changes only

Access and Use of Personally Owned Devices

NIST N 6103.24

Issue Date: 8/8/2016

Effective Date: 08/25/2003

PURPOSE

This directive defines requirements governing the use and connection of personally owned devices to NIST information systems in support of the NIST mission, while minimizing risks, promoting innovation and testing, facilitating communication and collaboration, and potentially reducing costs.

APPLICABILITY

This directive is applicable to all NIST information system users.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [Access and Use of Information Technology Resources O 6103.00](#);
- [Access and Use of IT While on Foreign Travel N6103.10](#);
- [DOC Safeguarding Data on Foreign Travel \(CITR-020\)](#);
- [Commerce Information Technology Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSPP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"](#) Access Control (AC) family.

DEFINITIONS

NIST Information System User – Any NIST employee or associate who enters into an agreement with NIST permitting their use of NIST Information Systems.

Personally owned devices – Any IT hardware that is owned by an individual and is not otherwise considered Government Furnished Equipment (GFE) or owned and supported by another organization. For example, IT hardware owned by NIST, DOC, other Federal agencies, vendor, contractors, or universities is not considered personally owned. IT hardware includes, but is not limited to, laptops, tablets, smartphones, memory sticks, smart cards, CDs, DVDs, hard drives, appliances, and servers.

REQUIREMENTS

1. Personally owned devices may be used in the contiguous United States in support of the NIST mission when NIST information accessed or stored is considered non-sensitive by management. Personally owned devices may not be used internationally in support of the NIST mission and may not connect to non-public NIST information systems while in a foreign country. In cases involving foreign travel, refer to separate guidance on obtaining an OISM approved foreign travel device in support of the NIST mission.
2. Personally owned devices may only be used with the NIST Remote Access Services and NIST networks specifically approved for such devices (e.g., NIST-Guest), so long as the service supports the device.
3. Personally owned devices may access NIST email services using NIST Remote Access Services, if the service supports the device operating system. However, to preserve email within the NIST email server, email must be accessed through a web browser, not a local email client which would otherwise store NIST email content locally.
4. Personally owned device owners are responsible for obtaining support from non-NIST service providers for personally owned device issues, applications installed on personally owned devices, or removing malware from personally owned devices.
5. The NIST IT Assistance Center (iTAC) and other NIST IT support staff shall not physically handle personally owned devices, and shall only provide limited support for network connectivity troubleshooting. Support limited to network connectivity shall only be provided when the device owner demonstrates:
 - a. all outstanding operating system critical patches have been successfully installed;
 - b. any installed peer-to-peer file sharing applications are disabled;
 - c. anti-virus software is installed, active (i.e., no expired trial versions) and has up-to-date definitions (if available); and
 - d. any virus incidents reported by anti-virus software have been quarantined or removed.

DIRECTIVE OWNER

18 - Office of Information Systems Management (OISM)

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Update	05/05/16	Islelly Castillo (OISM)	Ver. 2 Added additional requirements to the original directive
Update	06/23/16	Dan Cipra (M&O)	Formatting updates only
Rev..01	7/29/2016	Islelly Castillo (OISM)	Incorporated DRB Comments

Investigating Suspected Misuse of IT Resources

NIST O 6104.00

Issue Date: 8/7/2014

Effective Date: 01/01/2012

PURPOSE

The purpose of this directive is to ensure consistency, thoroughness, and objectivity in the conduct of forensic investigations of Information Technology (IT) misuse at NIST.

APPLICABILITY

This directive is applicable to all NIST management.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST information security directives](#);
- [Commerce Interim Technical Requirements](#);
- [DOC Information Technology Security Program Policy \(ITSP\)](#); and
- [NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"](#), Incident Response (IR) family;
- [NIST Special Publication 800-61, "Computer Security Incident Handling Guide"](#); and
- [NIST Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response"](#).

REQUIREMENTS

Misuse of IT Resources includes, but is not limited to the unacceptable and prohibited uses described in the Access and Use of IT Resources Directives.

1. Suspected misuse must be immediately reported to the NIST IT Security Officer (ITSO) or delegate.
2. Administration of a suspected misuse investigation and subsequent discipline or other appropriate follow-up actions must be completed expeditiously.
3. The Office of Information Systems Management (OISM) shall lead IT-related aspects of any investigations involving suspected misuse of IT resources at NIST.

- a) For incidents involving OISM staff, the NIST Chief Information Officer or Associate Director, Management Resources, will identify a team independent of OISM who will lead the investigation.
 - b) For incidents where delegation would not compromise the integrity of the investigation, OISM may delegate responsibilities to the impacted organizational unit (OU).
 - c) To avoid any appearance of partiality or bias, independence must be maintained between investigators and the individuals and organizations potentially involved.
 - d) OISM and delegated OU staff conducting investigations shall have the specialized skills, experience, and tools necessary to acquire and preserve information for potential evidentiary purposes, as identified for the Information System Security Incident Responder role in Commerce Interim Technical Requirement “Information System Security Training for Significant Roles” ([CITR-006](#)).
 - e) The investigative forensic process utilized shall follow NIST Special Publication [800-86](#).
4. Requests for employee or associate’s electronic communications or data shall be made to the Associate Director, Management Resources, in advance of any warranted action, except where such requests are from the DOC Office of the Inspector General and/or law enforcement.

RESPONSIBILITIES

NIST OU Management

- Request Associate Director, Management Resources approval for access to user electronic communications or data from systems, except telecommunications records which may be requested by OU management (i.e., Division Chief and above) through the IT Assistance Center.
- Report suspected misuse to the NIST ITSO.
- Administer appropriate discipline or other follow-up actions expeditiously in consultation with Office of Human Resources Management (OHRM) and other applicable NIST management.

Associate Director, Management Resources

- Approve or disapprove NIST management requests for employee or associate’s electronic communications or data, in advance of any warranted action, except where such requests are from the DOC Office of the Inspector General and/or law enforcement.

NIST IT Security Officer (ITSO)

- Lead IT-related aspects of investigations involving suspected misuse of IT resources.

- Promptly refer any IT misuse involving criminal activity to the DOC Office of the Inspector General and/or the appropriate law enforcement.
- Coordinate NIST employee misuse investigations with OHRM and respective OU management.
- Coordinate NIST Associate and other non-employee misuse investigations with the respective OU management.

Office of Human Resources Management (OHRM)

- Coordinate misuse investigations with NIST management, the NIST ITSO, and the Department of Commerce Office of General Counsel, as applicable.
- Advise NIST management on the administration of disciplinary or other follow-up actions as a result of misuse conducted by NIST employees.

DIRECTIVE OWNER

18 – Office of Information Systems Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft		Deb Dubeau	Original document
Ver. 0.01	7/10/14	Dan Cipra	Formatting updates

Position Sensitivity Levels for Information System Security

NIST O 6105.00

Issue Date: 8/7/2014

Effective Date: 8/7/2014

PURPOSE

The purpose of this directive is to define the minimum sensitivity and risk designations for positions with information system (IS) security responsibilities.

APPLICABILITY

This directive applies to staff serving in positions with IS security responsibilities.

REFERENCES

This directive is supplemental to a suite of security controls consisting of:

- [NIST Directive “Suitability and Fitness;”](#)
- [NIST information security directives;](#)
- [Commerce Interim Technical Requirements;](#)
- [DOC Information Technology Security Program Policy \(ITSPP\); and](#)
- [NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,”](#) Personnel Security (PS) family;
- [Clearance Requirements for DOC OU CIO and ITSO;](#)
- [U.S. Department of Commerce Manual of Security Policies and Procedures;](#)
- [Department Administrative Order DAO 202-731, “Position Sensitivity for Personnel Suitability and Personnel Security Purposes.”](#)

DEFINITIONS

Position Sensitivity Designations – Are given for national security positions and include the levels Special-Sensitive, Critical Sensitive and Non-critical Sensitive. See the U.S. Department of Commerce Manual of Security Policies and Procedures, Chapter 10, for further definition of these levels. When there are IS functions that relate to the potential sensitivity of a position, “IT” is appended to the sensitivity level. Note: IT (information technology) translates to ADP (Automated Data Processing) in the NIST [Automated Classification System](#) (ACS).

Position Risk Designations – Are given for all other positions and include the levels High, Moderate and Low Risk as defined in the DOC Manual of Security Policies and Procedures. When there are IS functions that relate to the potential risk associated with a position, “IT” is

appended to the risk level. Note: IT (information technology) translates to ADP (Automated Data Processing) in the NIST [Automated Classification System](#) (ACS).

System Categorization – Is determined by the highest rating for Confidentiality, Integrity, and Availability as stated in the NIST Information System Inventory.

REQUIREMENTS

1. Information system security positions must have the minimum position sensitivity and risk designation as shown in the table below. This information must be used in conjunction with relevant Department of Commerce Office of Security (OSY) and Office of Human Resources Management (OHRM) requirements.
2. NIST Management that provides supervisory or oversight functions for systems or systems staff must have a position sensitivity/risk rating that is appropriate for their level of access to the system and the information processed by the system.
3. Change of a non-IT level to an equivalent IT level (e.g., Low Risk to Low Risk IT) must be made the next time a position change is required (e.g., promotion, reassignment, statement of work, etc.).

Responsibilities or Role	System Categorization	Employee Minimum Position Sensitivity/Risk Designation	Minimum Designation of Non-Employee Positions ¹
System/Network Administrator for single user server, research laboratory server or research laboratory network Application/Database Administrator Information System Security Officer, Information System Owner, Authorizing Official	Low	Low Risk/Low Risk IT	Low Risk
	Moderate	Moderate Risk/Moderate Risk IT	Moderate Risk
	High	High Risk/High Risk IT	High Risk
	Classified Secret	Non-critical Sensitive/Non-critical Sensitive IT	Non-critical Sensitive
	Classified Top Secret	Critical Sensitive/Critical Sensitive IT	Critical Sensitive
Security Control Assessor, System/Network Administrator for	Low	Moderate Risk/Moderate Risk IT	Moderate Risk
	Moderate		
	High	High Risk/High Risk IT	High Risk

¹ Classified Contracts are handled under the auspices of the National Industrial Security Program.

production multi-user server (e.g., email server, web server, file server supporting multiple users) or production network	Classified Secret	Non-critical Sensitive/Non-critical Sensitive IT	Non-critical Sensitive
	Classified Top Secret	Critical Sensitive/Critical Sensitive IT	Critical Sensitive
OU IT Security Officer, Information System Security Incident Responders	Low	Non-critical Sensitive/Non-critical Sensitive IT	N/A
	Moderate		
	High		
	Classified Secret	Critical Sensitive/Critical Sensitive IT	N/A
	Classified Top Secret		
Chief Information Officer, Senior Information Security Officer, Chief Information Security Officer	Low	Special Sensitive/Special Sensitive IT	N/A
	Moderate		
	High		
	Classified Secret		
	Classified Top Secret		

RESPONSIBILITIES

NIST Management (e.g., Supervisors, Sponsors, and Contracting Officer's Representatives)

- Makes recommendations to OHRM on minimum risk and sensitivity levels for all employee positions under their authority having IS security responsibilities.
- Makes recommendations to OAAM on minimum designation for all contractor positions under their authority having IS security responsibilities.
- Ensuring minimum designation for all other associate positions under their authority having IS security responsibilities.

NIST Management (e.g., Information System Owner)

- Validate staff having responsibilities within an information system under their authority, has the appropriate minimum risk and sensitivity levels or designation.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	7/14/2014	Deb Dubeau	
Ver .01	7/14/2014	Dan Cipra	Formatting updates

Information Technology (IT) Compliance in Acquisition Checklist

NIST PR 6106.01
Effective Date: 10/20/2016

PURPOSE

This directive establishes procedures for the IT Compliance in Acquisition Checklist. The Checklist is a tool to help ensure that information technology (IT) acquisitions include the necessary provisions and protections along with terms and conditions.

APPLICABILITY

The Checklist applies to **all** types of Department of Commerce (DOC) **IT** acquisitions (new and renewed), including those made through or in support of assisted acquisitions associated with interagency agreements (IAA) where DOC is the requesting agency. The Checklist does not apply to micro-purchases acquired using a Government Purchase Card (GPC) unless the acquisition results in a new information system, or is deemed part of a national security system.

In addition to the criteria set forth in the Checklist, it is at the discretion of the Chief Information Officer (CIO) to require a Supply Chain Risk Assessment (SCRA) for any IT purchase.

REFERENCES

- [*44 U.S.C. Public Printing and Documents, Chapter 35, Coordination of Federal Information Policy*](#)
- [*Federal Acquisition Regulation \(FAR\)*](#)
- [*Federal Information Processing Standard \(FIPS\) 199, Standards for Security Categorization of Federal Information and Information Systems*](#)
- [*Commerce Acquisition Manual 1313.301 Department of Commerce Purchase Card Program*](#)
- [*IT Compliance in Acquisition Checklist Requirements \(Memorandum dated June 15, 2016, issued by DOC Chief Information Officer\)*](#)
- [*Commerce Interim Technical Requirements \(CITR\) - 019, Risk Management Framework*](#)
- [*Commerce Interim Technical Requirements \(CITR\) - 023, Pre-Acquisition Supply Chain Risk Assessment*](#)

- [DOC Procurement Memorandum 2015-08, Supply Chain Risk Assessment \(SCRA\) Requirements for the Acquisition of Moderate-Impact and High-Impact Information Systems, dated September 30, 2015](#)
- [NIST Special Publication \(SP\) 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations](#)
- [NIST Acquisition Management Division Standard Operating Procedure 07-13: Package Receipt and Verification Process](#)
- [O 6106.00 Policy on Acquisition Development and Support of Information Technology Applications and Systems](#)

DEFINITIONS

Information Technology (IT) and/or Information System

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, and is subsequently subject to the reporting requirements of 44 U. S. C. Section 3505(c)2 FISMA Reportable System.

- A **new** information system is one in which a new system inventory record will be created and entered into the NIST Information System Inventory.
- A **significant change** to an information system is an alteration which may have a considerable effect on the security of the information and/or system, or that directly affects the security management of the system.

Information Technology (IT) - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Electronic and Information Technology (EIT) – Electronic and information technology (EIT) has the same meaning as “information technology” except EIT also includes any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The term EIT includes, but is not limited to, telecommunication products (such as telephones), information kiosks and transaction machines, worldwide websites, multimedia, and office equipment (such as copiers and fax machines).

Information and Communications Technology (ICT) - Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.

National Security System - Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

ICT Supply Chain Risk Management - The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.

ICT Supply Chain Risk Assessment (SCRA) - Process to identify risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

ICT Supply Chain Criteria – The characteristics of an IT system acquisition that prompt an ICT Supply Chain Risk Assessment. Characteristics include: (1) an information system that the Department designates as FIPS 199 high or moderate- impact system; **and** (2) that is subject to the reporting requirements of 44 U. S. C. Section 3505(c)2 FISMA Reportable System; **and** (3) for which a new system inventory record will be created and entered into the CSAM in accordance with CTR-019 Risk Management Framework (RMF).

Service – a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks

Service Level Agreement – an agreement between a service provider and a customer

RESPONSIBILITIES

NIST Chief Information Officer (CIO)

- Oversees information technology services and systems, and ensures compliance with Federal IT Regulations and DOC/NIST IT security requirements.
- Determines the need for a SCRA for new information technology and information systems.
- Designates the CO to coordinate with DOC when an SCRA is needed.
- Delegates the review of acquisitions containing IT to the OU ITSO.
- Communicates the outcome of the SCRA to appropriate parties.

NIST IT Security Officer (NIST ITSO)

- Oversees the NIST IT security program, including IT security aspects for the acquisition of new IT and information systems.
- Reviews information system impact requirements determined in accordance with Federal IT Security Regulations and DOC/NIST IT security requirements.
- Supports the CIO by identifying new information systems or information technology that require a SCRA.

OU Information Technology Security Officer (OU ITSO)

- Determines whether an acquisition contains IT.
- Reviews the IT Compliance in Acquisitions Checklist for all proposed IT procurements.
- Identifies new information systems or information technology that may require a SCRA.
- Serves as the primary point of contact for the OU for IT security matters related to acquisitions.
- Delegates responsibilities above, in whole or in part, to a formally trained security professional (e.g., ISSO).

Information System Security Officer (ISSO)

- Serves as the technical point of contact for information security matters for assigned information system(s).
- Fulfills responsibilities of OU ITSO, in whole or in part, as designated by OU ITSO.

Director of the Office of Acquisition and Agreements Management (OAAM)/Senior Bureau Procurement Official (SBPO)

- Oversees acquisitions and agreements, and ensures compliance with Federal Acquisition Regulations and DOC/NIST acquisition policies and procedures.

Government Purchase Card Requestor

- Identifies procurement requirements.
- Provides sufficient information pertaining to acquisition and collaborates with their assigned OU ITSO to determine whether or not an acquisition is a service that includes information technology (IT) and/or product that includes information technology (IT).

Procurement Requestor

- Identifies procurement requirements.
- Provides sufficient information pertaining to acquisition and collaborates with their assigned OU ITSO to determine whether or not an acquisition is a service that includes information technology (IT) and/or product that includes information technology (IT).

- Completes the IT Compliance in Acquisitions Checklist and submits the Checklist with the acquisition documentation, to the OU ITSO for review and approval if the purchase includes IT.

Contracting Officer's Representative (COR)

- Completes and reviews the IT Compliance in Acquisition Checklist in coordination with the OU ITSO.

Contracting Officer (CO)

- Ensures that the completed and appropriately signed IT Compliance in Acquisitions Checklist is included in the Procurement Request file.
- Collects, coordinates, and submits required information for SCRA, if applicable. Ensures that applicable provisions and clauses are included in solicitation and contract documentation.
- Applies appropriate provisions and clauses in the solicitation and contract documentation based on responses to the completed IT Compliance in Acquisitions Checklist.

Program Manager

- Identifies acquisition requirements when using interagency agreement funding.
- Provides sufficient information pertaining to acquisition and collaborates with their assigned OU ITSO to determine whether or not an acquisition is a service that includes information technology (IT) and/or product that includes information technology (IT).
- Completes the IT Checklist and collaborates with RACO to integrate appropriate procurement requirements in the assisted acquisitions associated with interagency agreement documentation if the purchase includes IT.

Reimbursable Agreements Coordination Office (RACO)

- Coordinates all terms and conditions, to include those required by the IT Checklist and SCRA determination requirements, for IT procurements included in the NIST payable agreements.

PROCEDURES

- I. Government Purchase Card Requestor, Procurement Requestors, and Program Managers must collaborate with their assigned OU ITSO to determine whether or not an acquisition is a service and/or product that includes information technology (IT).
 - A. The Government Purchase Card may not be used for the acquisition of IT deemed part of a National Security System (NSS).
 - B. If the request includes IT, then their assigned OU ITSO must determine whether the acquisition meets the ICT supply chain criteria.

- i. If an acquisition meets the criteria for creating a new information system or creating a significant change, then the Government Purchase Card shall not be used to complete the transaction, per section 4 of Procurement Memorandum 2015-08, dated September 30, 2015.
 - ii. If an acquisition does not meet the ICT supply chain criteria, then either a Government Purchase Card, Procurement Request, or Interagency Agreement may be used, contingent upon the regulations associated with each.
 - C. If the request does not include IT or is a micro-purchase being acquired using a Government Purchase Card, and is not part of a national security system, then the IT Compliance in Acquisitions Checklist is not applicable.
- II. If using a **Procurement Request** for an acquisition that includes IT, prior to purchase, the following applies:
 - A. Requestor to review and complete Questions 1-4.
 - B. Requestor to review and complete Question 5, Part I (5A), which cites the conditions under which the acquisition will require submission of a supply chain risk assessment (SCRA)
 - i. If NO for Question 5, Part I (5A), an SCRA is NOT required.
 - ii. If YES for Question 5, Part I (5A), an SCRA is required.
 - C. Requestor to review and complete Question 5, Part II (5B and 5C).
 - i. Question 5, Part II (5B)
 - a. If NO, an SCRA is NOT required.
 - b. If YES, proceed to (5C).
 - ii. Question 5, Part II (5C)
 - a. If NO, an SCRA is required.
 - b. If YES, an SCRA is NOT required.
 - iii. The OU OCIO Point of Contact for Question 5 is delegated per CITR-023, section 6.2.1, to the Requestor's assigned OU-level IT Security Officer.
 - iv. Requestor to review and complete Question 6, if applicable.
- III. If using **Interagency Agreement** funding for an acquisition that includes IT:
 - A. Where NIST is the requesting agency (*transferring funds to another agency*), the NIST Program Manager must complete the following prior to agreement submission to [NIST Reimbursable Agreements Coordination Office \(RACO\)](#):

- i. Follow the process described above in section 2 as appropriate to complete the IT Checklist and SCRA determination. Submit that information to RACO with the agreement package.
 - ii. Coordinate with RACO to develop applicable terms and conditions for the agreement based on responses to the completed IT Compliance in Acquisition Checklist and SCRA determination.
 - B. Where NIST is the servicing agency (*receiving funds*), the Program Manager will serve as the Procurement Requestor and must follow the process described above in section 3 as appropriate to complete the IT Checklist and SCRA determination.
- IV. If an SCRA is required:
 - A. The Requestor must submit a complete procurement package through their assigned OU ITSO, the NIST ITSO, and thereafter submitted to the Contracting Officer;
 - B. The Contracting Officer will coordinate with the requisite parties to:
 - i. Obtain offeror information (see Contract Language from Procurement Memorandum 2015-08); and
 - ii. Complete and submit a supply chain risk assessment (SCRA) and transmittal memorandum, as a supplemental document to the Checklist. (See information detailed in the Supply Chain Risk Assessment Information, section 5.c. of the DOC Procurement Memorandum 2015-08).
- V. Requestor to obtain review and approval as follows:
 - A. Checklist Signatures

Signature cited on form:	Equivalent to:
Cognizant OCIO Representative, if applicable - Signature only necessary if SCRA is required.	Chief Information Officer, Deputy Chief Information Officer, or NIST IT Security Officer
Information System Security Officer (ISSO)	Requestor's OU IT Security Officer (<i>if delegated, Requestor's assigned ISSO</i>)
Procurement COR	Procurement Requestor or proposed Contracting Officer's Representative (COR), or Program Manager
Organizational Unit approved Program/Requesting Office IT Security Officer	Requestor's assigned OU IT Security Officer (<i>if delegated, Requestor's assigned ISSO or other trained security professional</i>)

Contracting Officer	Contracting Officer, if applicable

- VI. The completed checklist must be maintained with the Requestor/Procurement Requestor/Program Manager's documentation (e.g., transaction file, contract file, etc.).
- VII. For purchases made through the IT Buying Service, Managed Mobile Device Service, and Microsoft Enterprise Agreement (i.e., NIST-wide strategic sourcing vehicles):
 - A. OISM must complete the IT Compliance in Acquisition Checklist, and host a copy in its Knowledge Base for NIST customer reference.
 - B. Purchases made by NIST customers through OISM do not require a separate IT Compliance in Acquisitions Checklist, but require reference to the Checklist.
 - C. OISM must complete a new Checklist when a new strategic sourcing vehicle goes into effect.
- VIII. Each OU may define a process for the use of the Checklist, and may use electronic signature for processing of the Checklist. However, OU defined processes must meet requirements defined in the [NIST Directive on the Use of Electronic Signatures](#).
- IX. The most recent version of the IT Compliance in Acquisitions Checklist (version 3.5) must be used, as applicable.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial		Carol Schmidt	Draft
Rev. .01	8/22/2016	Dan Cipra	Formatting updates only
Rev. .02			

Management of Windows and Macintosh Computers

NIST O 6110.00

Issue Date: 12/23/2014

Effective Date: 12/23/2014

PURPOSE

This directive defines requirements for the purchase and management of networked, NIST-owned Windows and Macintosh computers.

The objective of this order is to ensure that all NIST organizational units maintain their Windows and Macintosh computers in a secure manner as cost effectively as possible. In order to comply with the Federal Information Security Management Act (FISMA), computers must be properly secured in conformance with secure configuration standards. Initially deploying computers with standard images, and centrally managing configuration updates with automated tools is more reliable and less costly than securing computers one by one. Support is also faster and more cost effective, because the desktop support team has certified Dell and Apple technicians and maintains stocks of replacement parts, and the managed desktop services allow support technicians to remotely diagnose and fix many problems.

APPLICABILITY

This directive applies to all NIST-owned Windows and Macintosh computers used in the conduct of NIST business, with the exception of devices on the Research Equipment Network (REN) and non-networked devices.

REFERENCES

- [Department of Commerce \(DOC\) Information Technology Portfolio Management Policy](#);
- [Department Organization Order \(DOO\) 30-2B](#), Section 6.04, The Office of Information Systems Management;
- [OMB Circular No. A-130 Revised](#), Memorandum for Heads of Executive Departments and Agencies on Management of Federal Information Resources;
- Clinger-Cohen Act (also known as "[Information Technology Management Reform Act of 1996](#)"), Public Law (P.L.) 104-106, Division E;
- [E-Government Act of 2002](#), Public Law (P.L.) 107-347; and
- Memorandum from DOC Deputy Secretary entitled "[Department-wide contract for Personal Computers and Accessories](#)" dated March 23, 2012.

- OMB Memo M-14-04 [Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management](#)

REQUIREMENTS

1. All new NIST-owned Windows laptops, desktops, Ultrabooks and monitors must be purchased through the [IT Buying Service](#).
2. All new NIST-owned Windows and Macintosh computers on the NIST network must be configured by the Office of Information Systems Management.
3. All NIST-owned Windows and Macintosh computers on the NIST network must authenticate to the campus.nist.gov (NIST) domain.
4. All NIST-owned Windows and Macintosh computers on the NIST network must participate in the managed desktop services provided by the Office of Information Systems Management.
5. Waiver requests for these requirements must follow procedures located at: https://inet.nist.gov/oism/howdoi/iss_waivers.cfm. The purchase of any Windows laptop, desktop, Ultrabook or monitor not listed on the Buying Service website must have a justification approved by the NIST Procurement Official or Designee before the purchase is made using the “Non-Use of DOC Custom User Purchasing Agreement (CUPA)” form. Waiver requests for the other three requirements must be approved by the NIST Information Technology Security Officer (ITSO), using the “Management of Windows and Macintosh Computers” form.

RESPONSIBILITIES

NIST Information Technology Security Officer (ITSO)

- Approve waivers for Windows and Mac computers that cannot comply with this policy to be on the NIST network.

NIST Bureau Procurement Official (BPO)

- Approve justification for purchase of any laptop, desktop, monitor or accessory not listed on the IT Buying Service.

OU IT Security Officer

- Recommend approval of waivers to this directive in cases where a user’s work responsibilities cannot be accomplished while meeting these requirements.
- Forward completed waiver request to the NIST ITSO for approval.

Information System Owner

- Recommend approval of waivers to this directive in cases where a user’s work responsibilities cannot be accomplished while meeting these requirements.

Computer Users

- Ensure that the computer authenticates to the NIST domain.
- Reboot the computer when requested to allow patches to be implemented.

- If a user believes that his/her work responsibilities cannot be accomplished while meeting these requirements, he/she must have a waiver approved by the NIST ITSO.

DIRECTIVE OWNER

18 - Office of Information Systems Management

APPENDICES

A. Revision History

Appendix A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Rev 2	10/2/14	Susannah Schiller	Revised scope to explicitly exclude non-networked computers as well as those on the REN, and added NIST CISO to approvers for waivers.
Rev 3	10/17/14	Susannah Schiller	Referenced the CUPA justification for the purchase of equipment not on the CUPA. This is an update from referring to the NIST buying service.
Rev 4	12/19/14	Dan Cipra	Accepted all DRB comments and finalized.

Occupational Safety and Health

NIST P 7100.00
Effective Date:¹ 8/2/2016

PURPOSE

To articulate NIST's commitment to protecting NIST employees, associates, and visitors from NIST workplace hazards.

SCOPE

This policy applies to NIST employees and covered associates² at any NIST workplace.

LEGAL AUTHORITY

- [Occupational Safety and Health Act of 1970](#), as amended, 29 United States Code (U.S.C.) § 651 et seq.
- [Executive Order \(E.O.\) 12196](#), Occupational Safety and Health Programs for Federal Employees (1980)
- [Department of Commerce Organization Order 30-2A](#), National Institute of Standards and Technology

POLICY

It is NIST policy to carry out all activities in a manner that protects employees, associates, and visitors from occupational injury and ill health due to NIST workplace hazards. Considering safety to be the control of recognized hazards to achieve an acceptable level of risk, NIST is committed to making occupational safety and health an integral core value and vital part of the NIST culture by:

- Integrating safety and health considerations systematically into work practices at all levels, including all aspects of work planning and execution;
- Providing the resources necessary for employees and covered associates to conduct their work safely;
- Engaging employees and covered associates in safety and health matters;
- Fostering a work environment in which employees and covered associates are encouraged to report and raise safety and health issues without fear of retaliation;

¹ For revision history, see Appendix A.

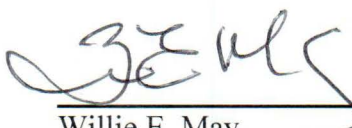
² Any associate other than a non-research-and-development contractor. For detailed definitions of "Associate", "Covered Associate", and "Non-R&D Contractor", see [NIST O 7100.01, Occupational Safety and Health Management System](#).

- Continually improving the effectiveness and efficiency of NIST's safety and health processes, systems, and capabilities through assessments and other mechanisms;
- Complying with applicable laws, regulations, and other promulgated safety and health requirements; and
- Setting and communicating occupational safety and health objectives.

In addition, every employee and covered associate at NIST is expected to:

- Take personal responsibility for their own safety by:
 - Ensuring that they have and use the knowledge, skills, abilities, and equipment to work safely at all times;
 - Never working under unsafe conditions at any workplace or on travel; and
 - Remaining vigilant in all of their activities; being aware of the safety consequences of their actions and taking care to minimize any adverse consequences.
- Take personal responsibility for the safety of others by:
 - Respectfully challenging one another – and accepting challenges – on unsafe behavior;
 - Taking action and lending their expertise to assist others in being safe;
 - Taking actions when there is an injury or illness;
 - Communicating with their co-workers on matters that may affect their well-being; and
 - Ensuring visitors are aware of and follow necessary safety precautions.
- Take personal responsibility for making safety an integral core value and vital part of the NIST culture by:
 - Promptly reporting incidents;
 - Participating in the conduct of incident investigations;
 - Promptly reporting or otherwise addressing unsafe or unhealthful working conditions;
 - Sharing safety information and lessons learned; and
 - Correcting deficiencies and taking actions to prevent incidents from occurring.

The Associate Director for Management Resources shall ensure the development of other directives necessary for the full and effective implementation of this policy.


 Willie E. May
 Director

AUG 02 2016

Date

Appendix A

Revision History

Revision No.	Issue Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	09/05/2012	NA	09/05/12	<ul style="list-style-type: none">Initial document approved by NIST Director Patrick D. Gallagher
1	07/24/2015	NA	07/24/15	<ul style="list-style-type: none">Initial document re-approved by NIST Director Willie E May
2	8/2/2016	NA	8/2/16	<ul style="list-style-type: none">Made the policy applicable to “Covered Associates”Clarified purpose and scope

Occupational Safety and Health Management System

NIST O 7101.00

Approval Date: 8/2/2016

Effective Date:¹ 8/2/2016

PURPOSE

Define the requirements of the NIST occupational safety and health management system (OSHMS) necessary for the full and effective implementation of NIST P 7100.00, Occupational Safety and Health (OSH), together with the roles and responsibilities of NIST employees and covered associates in meeting those requirements.

SCOPE

The scope of the NIST OSHMS comprises NIST P 7100.00, this order, and the OSH directives, deployment tools, and Organizational Unit (OU) procedures necessary to implement this order.

APPLICABILITY

This issuance is applicable to NIST employees and covered associates at any NIST workplace.

REFERENCES

- [Occupational Safety and Health Act of 1970](#), as amended, 29 United States Code (U.S.C.) § 651 et seq.
- [Executive Order \(E.O.\) 12196](#), Occupational Safety and Health Programs for Federal Employees (1980)
- [29 Code of Federal Regulations \(CFR\) Part 1904](#), Recording and Reporting Occupational Injuries and Illness
- [29 CFR Part 1960](#), Basic Program Elements for Federal Employee Occupational Health and Safety Programs and Related Matters
- Occupational Health and Safety Assessment Series (OHSAS) Standard 18001:2007, Occupational Health and Safety Management Systems – Requirements
- [NIST Policy 7100.00, Occupational Safety and Health](#)
- [NIST Executive Safety Committee \(ESC\) Charter](#)

¹ For revision history, see Appendix A.

REQUIREMENTS

NIST shall comply with the requirements of E.O. 12196, 29 CFR Part 1960, and OHSAS Standard 18001:2007. These requirements include:

NIST Director shall:

- Define and authorize NIST's OSH policy
- Take ultimate responsibility for OSH and the OSHMS
- Demonstrate their commitment by ensuring the availability of resources essential to establish, implement, maintain, and improve the OSHMS
- Define roles, allocate responsibilities and accountabilities, and delegate authorities to ensure that requirements, including the following, are met:
 - Procedures are established, implemented, and maintained for ongoing hazard identification; risk assessment; determination, implementation, and maintenance of necessary controls; and immediate incident response
 - The OSH hazards and OSH risks associated with changes in the organization, its activities, or the OSHMS are identified prior to the introduction of such changes
 - Procedures are established, implemented, and maintained for identifying and accessing the regulatory and other OSH requirements that are applicable to NIST and for ensuring that these are taken into account in establishing, implementing and maintaining the OSHMS
 - Documented OSH objectives and plans for achieving those objectives are established, implemented, and maintained
 - Persons in the workplace are assigned responsibility for aspects of OSH over which they have control, including adherence to applicable OSH requirements
 - Any person under NIST's control performing tasks that can impact OSH have appropriate safety education, training, or experience
 - Procedures are established, implemented, and maintained for the participation, as appropriate, of employees and covered associates in hazard identification, risk assessment, and determination of controls; incident investigation; and development and review of the OSHMS
 - Procedures are established, implemented, and maintained to monitor and measure OSH performance on a regular basis
 - Procedures are established, implemented, and maintained for periodically evaluating compliance with applicable regulations and other requirements

- Procedures are established, implemented, and maintained for recording and investigating incidents, for analyzing incident data, and for taking corrective and preventive actions to avoid recurrence
- Procedures are established, implemented, and maintained for dealing with actual and potential nonconformities and for taking corrective and preventive actions
- Records are established and maintained as necessary to demonstrate conformity by NIST to the requirements of the OSHMS and the results achieved
- Internal audits of the OSHMS are conducted at planned intervals
- Review the organization's OSHMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness

NIST Managers and Supervisors shall:

- Demonstrate their commitment to the continual improvement of OSH performance

DEFINITIONS

Associate – An individual conducting work at a NIST workplace who is not a NIST employee. For a list of NIST associate types, click [here](#).

Audit – Systematic, independent, and documented process for obtaining “audit evidence” and evaluating it objectively to determine the extent to which “audit criteria” are fulfilled. NOTE: “Independent” does not necessarily mean external to the organization. In many cases, independence can be demonstrated by the freedom from responsibility for the activity being audited.

Authority Having Jurisdiction – A Fire Protection Engineer in the Office of Safety, Health, and Environment (OSHE) designated by the Chief Safety Officer (CSO) to enforce the NIST-adopted codes and standards relevant to fire, electrical, and life safety on NIST-owned and operated sites.

Common Spaces within a Building – Spaces within a building, including lobbies, corridors, stairwells, elevators, restrooms, break rooms, and loading docks, that are open to building occupants and to the occupants of other buildings. Common spaces may or may not be assigned to an OU in the NIST space management system. See definition of “OU Space”.

Corrective Action – Action to eliminate the cause of a detected nonconformity or other undesirable situation.

Covered Associate – A NIST associate permitted to perform work at a NIST workplace and subject to NIST policies and procedures to the extent allowed by law and the terms of the associate’s agreement. Covered associates include Foreign and Domestic Guest Researchers (including contractors who perform NIST R&D/technical work); Research Associates;

Intergovernmental Agency Personnel Act assignees; Facility Users; Volunteer Students; and other federal employees who perform work at NIST workplaces.

Document – Written information and its supporting medium.

Effective Date (of an OSH Directive) – The date upon which the requirements of a directive enter into force. See definition of “Issue Date”.

Employee – For the purposes of this order, the term “Employee” refers to an individual who is (a) appointed in the civil service by the NIST Director acting in an official capacity, (b) engaged in the performance of a Federal function under authority of law or an Executive act, and (c) subject to the supervision of the NIST Director or an individual named by paragraph (a) while engaged in the performance of the duties of his position (see 5 U.S.C. 2105).

Hazard – Source, situation, or an act with a potential for harm in terms of human injury or ill health, adverse impact on the environment, damage or loss of equipment or property, or a combination of these.

Hazard Identification – Process of recognizing that a hazard exists and defining its characteristics.

Ill Health – Identifiable, adverse physical or mental condition arising from or made worse by a work activity or work-related situation (OHSAS Standard 18001:2007; see definition of “Work Related”).

Implement (an OSH Directive or OU Procedure) – Ensure that the requirements of the OSH directive or OU procedure are met.

Incident – A work-related event in which any of the following, individually or in combination, occurred or could have occurred: an injury or illness; an unauthorized spill or release of hazardous or regulated material to the environment; damage or loss of equipment or property. The “could have occurred” situation corresponds to “near misses”, defined below.

Interested Party – Person or group, inside or outside the workplace, concerned with or affected by the OSH performance of an organization.

Issue Date (of an OSH Directive) – The date an OSH directive is published in the NIST Directives Management System. See definition of “Effective Date”.

Near Miss – Also known as a “near hit,” “near-accident,” or “close call,” an incident that did not result in any of the following, either individually or in combination, but had a plausible likelihood of doing so: a work-related injury or illness; a spill or release of hazardous or regulated material to the environment; damage or loss of equipment or property.

NIST Workplace – An establishment at one geographical location at which work-related activities are conducted by NIST employees or covered associates. NIST workplaces include sites owned and operated by NIST and by other organizations.

Nonconformity – Non-fulfillment of a requirement.

Non-R&D Contractor – A NIST associate who performs non-R&D work at a NIST workplace in accordance with the safety requirements of a contract or other legal arrangement, such as a Memorandum of Understanding, with NIST. Non-R&D contractors include, but are not limited to, construction contractors; facilities contractors; equipment installation, service, and maintenance contractors; Health Unit contractors; contract cafeteria workers; and janitorial contractors.

Occupational Safety and Health (OSH) – Conditions and factors that affect, or could affect, the health and safety of employees, associates, visitors, or any other persons in the workplace. See Occupational Health and Safety Assessment Series (OHSAS) Standard 18001:2007.

Organizational Unit (OU) – Term used herein to denote any of the following: Office of the NIST Director; the immediate office of a NIST Associate Director; a NIST Laboratory; a NIST Extramural Program; or a NIST Chief Office.

OSH Deployment Tools – Tools, such as forms, instructions, IT applications, training, and user guides, developed by OSHE to facilitate the implementation of OSH directives.

OSH Management System (OSHMS) – Part of an organization's management system used to develop and implement its OSH policy and manage its OSH risks. NOTE: A management system is a set of interrelated elements used to establish policy and objectives and to achieve those objectives. It includes organizational structure, planning activities (including, for example, risk assessment and the setting of objectives), roles and responsibilities, practices, procedures, processes, and resources.

OSH Objective – OSH goal, in terms of OSH performance, that an organization sets itself to achieve.

OSH Performance – Measurable results of an organization's management of its OSH risks. OSH performance measurement includes measuring the effectiveness of the organization's controls. In the context of OSH management systems, results can also be measured against the organization's OSH policy, OSH objectives, and other OSH performance requirements.

OSH Policy – Overall intentions and direction of an organization related to its OSH performance as formally expressed by the NIST Director; for NIST, NIST P 7100.00, Occupational Safety and Health.

OSH Program – An OSH suborder; all supporting suborder-specific directives, including procedures, guidance, and notices; and any associated OSH deployment tools and OU procedures.

OSH Program Manager – For a given OSH program, an OSHE staff member assigned by the CSO to manage that program.

OSH Suborder – A technical document that significantly expands on one or more aspects of an OSH order.

OU Activity – An activity conducted by employees and covered associates from a single OU, or, when an activity is conducted by employees and covered associates from multiple OUs, an activity assigned to a particular OU by agreement among the participating OUs.

OU-Assigned Building – A building in which an OU has full-time building occupants *and* either that OU has the most OU space in that building based on the information in the NIST space management system managed by the Office of Facilities and Property Management (OFPM), or the OUs with full-time building occupants have agreed, in writing, that the building will be assigned to another of those OUs. NOTE: This definition is used herein only to assign responsibility for OSH management of common spaces in buildings to OUs; it is not intended to imply that buildings are assigned by OFPM to OUs.

OU/Division Safety Personnel – Employees, such as OU Safety Coordinators and Division Safety Representatives, who have been designated by their OUs or divisions to perform OSH-related duties on behalf of their OUs/divisions on a full- or part-time basis.

OU Space – Space assigned to an OU in the NIST space management system maintained by OFPM, space in an adjacent service galley and considered an extension of such space, or space loaned to an OU by another OU on a non-permanent basis.

Preventive Action – Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.

Procedure – Specified way to carry out an activity or a process. The OSHMS may or may not require a procedure be written.

Record – Document stating results achieved or providing evidence of activities performed. (OHSAS Standard 18001:2007; this definition is narrower than that in 44 U.S.C. 3301).

Risk – Combination of the likelihood of an occurrence of a hazardous event or exposure and the severity of injury or ill health that can be caused by the event or exposure.

Risk Assessment – Process of evaluating the risks arising from hazards, taking into account the adequacy of any existing controls, and deciding whether or not the risks are acceptable.

Shall/Should/May –

- Shall (Must or Will): Indicates that the performance of an item is mandatory.
- Should: Indicates that the performance of an item is not mandatory, but the full implications of not performing that item must be understood and either justified or carefully weighed before choosing a different course.
- May: Indicates that the performance of an item is at the discretion of the individual responsible for the action.

Visitor – Any individual at a NIST workplace who is sponsored by a NIST employee or associate but who is not a NIST employee or associate.

Work Related – A condition wherein an injury, illness, or fatality was caused, contributed to, or significantly aggravated, or could have been, by an event or exposure at work or on official business away from work (see 29 CFR 1904.5).

ACRONYMS

AHJ – Authority Having Jurisdiction

CFR – Code of Federal Regulations

CSO – Chief Safety Officer

EO – Executive Order

ESC – Executive Safety Committee

NCNR – NIST Center for Neutron Research

OFPM – Office of Facilities and Property Management

OSH – Occupational Safety and Health

OSHE – Office of Safety, Health, and Environment

OSHMS – Occupational Safety and Health Management System

OU – Organizational Unit

U.S.C. – United States Code

RESPONSIBILITIES

The following roles and responsibilities apply to this order and all OSH suborders. Suborders for specific OSH programs may contain additional roles and responsibilities.

NIST Director

- Ensure the development, implementation, maintenance, and continual improvement of the NIST OSHMS in accordance with the requirements of OHSAS Standard 18001:2007
- Define the roles, responsibilities, and accountabilities and delegate authorities to facilitate effective OSH management
- Ensure the availability of resources essential to develop, implement, maintain, and continually improve the OSHMS at all operational levels
- Provide direction as necessary on significant issues involving OSH and regulatory compliance
- Ensure the implementation of accountability and enforcement policies in support of OSH and regulatory compliance

- Ensure that employees and covered associates are not subject to restraint, interference, coercion, discrimination, or reprisal for reporting hazardous situations or participating in OSH program activities
- Approve the ESC charter

NIST Director and Associate Directors (as a group)

- Review the OSHMS no less frequently than every two years to ensure its continuing suitability, adequacy, and effectiveness
 - Assess opportunities for improvement and the need for changes to the OSHMS based on:
 - The results of internal audits and evaluations of compliance with applicable regulatory and other requirements to which NIST subscribes
 - The results of participation and consultation
 - Relevant communications from external interested parties, including complaints
 - The OSH performance of the organization, including consideration of the factors causing incidents and the extent to which OSH objectives have been met
 - Status of incident investigations, corrective actions and preventive actions
 - Follow-up actions from previous management reviews
 - Changing circumstances, including developments in regulatory and other requirements related to OSH recommendations for improvement
 - Make decisions and direct actions related to possible changes to:
 - OSH performance
 - OSH policy and objectives
 - Resources
 - Other elements of the OSHMS

NIST Associate Directors (as individuals)

- Assist the NIST Director in carrying out their responsibilities
- Ensure the implementation of the NIST OSHMS in their respective directorates
- Monitor, ensure, and enforce the implementation of accountability in support of OSH and regulatory compliance
- Review the ESC charter

Associate Director for Management Resources (in addition to the responsibilities above of all NIST Associate Directors)

- Ensure the development of the OSH suborders, other directives, and deployment tools necessary for the full and effective implementation of NIST P 7100.00 and this order

CSO (in addition to the responsibilities below of all other OU Directors)

General

- Assist the NIST Director in the development, implementation, maintenance, and continual improvement of the NIST OSHMS in accordance with the requirements of OSHMS Standard 18001:2007
- Carry out their responsibilities in partnership with customers and stakeholders
- Establish, implement, and maintain an OSH program development, deployment, and maintenance program for establishing, deploying, and maintaining the OSH programs necessary for the full and effective implementation of this order
- Designate an OSHE employee to serve as the AHJ
- Designate OSHE employees to serve as OSH Program Managers for NIST's OSH programs
- Ensure that the AHJ and OSH Program Managers have the authority, resources, and training necessary to carry out their responsibilities.
- Ensure that the OSHE staff provides high-quality OSH services

Regulatory and Other Requirements

- Establish, implement, and maintain procedures for identifying and accessing OSH regulatory and other requirements
- Take OSH regulatory and other requirements into account in establishing and maintaining the OSHMS
- Keep OSH regulatory and other requirements up-to-date and communicate them to employees, covered associates, and other interested parties
- Ensure that OSH directives that require OUs to develop, implement, and maintain written procedures delineate the specific requirements that those procedures must meet

Hazard Identification, Risk Assessment, and Determination and Implementation of Controls

- Establish and maintain a hazard review program to address:
 - Ongoing hazard identification
 - Risk assessment
 - Determination, implementation, and maintenance of necessary controls
 - Immediate incident response

- Establish and maintain management of change and hierarchy of controls programs
- Establish and maintain OSH programs to integrate into the overall OSHMS the operational controls necessary to manage the OSH risks associated with specific types of hazard (e.g., biological, chemical, electrical, optical, stored hazardous energy)
- Establish and maintain OSH programs to integrate into the overall OSHMS the operational controls necessary to manage the OSH risks associated with:
 - Procurement of goods
 - Transfer of NIST materials, equipment, and devices to other organizations
 - Minors working at NIST
 - Non-R&D contractors
 - Visitors

Competence, Training, and Awareness

- Establish and maintain a safety education and training program, integrated with other programs as appropriate, to ensure that employees and covered associates are provided the safety education, training, and experience needed to carry out their work at NIST safely.

Communication, Participation, and Consultation

- Establish, implement, and maintain procedures for internal communication among the various management levels and functions at NIST with regard to OSH hazards and the OSHMS
 - Ensure that reports on the performance of the OSHMS are presented to the NIST Director, Associate Directors, and OU Directors for review
- Establish, implement, and maintain procedures for the participation of employees and covered associates in the development and review of the OSHMS and OSH objectives
- Engage the ESC and other groups as appropriate in the development and review of the OSHMS and OSH objectives
 - Chair the ESC in accordance with its charter
 - Develop and maintain the ESC charter
- Establish, implement, and maintain procedures for receiving, documenting, and responding to relevant communications from external parties, including regulatory agencies and officials
- Ensure, when appropriate, that relevant external parties are consulted about pertinent OSH matters

Document and Record Control

- Ensure that OSHMS documentation includes documents required by the OSHMS and determined to be necessary to ensure the effective planning, operation, and control of processes that relate to the management of OSH risks
- Establish, implement, and maintain a document and record control program for controlling documents, including records, required by the OSHMS

Performance Measurement and Monitoring, Assessments, Incident Reporting and Investigation, and Corrective and Preventive Actions

- Establish, implement, and maintain a performance measurement and monitoring program to monitor and measure OSH performance on a regular basis
- Ensure that reports on the performance of the OSHMS are used as a basis for improvement of the OSHMS
- Establish, implement, and maintain an assessment program for periodically evaluating compliance with applicable legal and other requirements and for conducting internal audits of the OSHMS at planned intervals
- Ensure that written OU procedures required by OSH directives are reviewed by OSHE to verify that they meet the requirements delineated in the directives and provide the results of those reviews to the OU Directors
- Establish and maintain an incident reporting and investigation program to record, investigate, and analyze incidents and communicate lessons identified
- Establish and maintain a program for reporting, investigating, and abating working conditions that are, or may be, unsafe or unhealthful to employees, covered associates, or visitors or harmful to the environment
- Establish and maintain a corrective and preventive action program for addressing actual and potential nonconformities through corrective and preventive actions

Management Review and Planning

- Develop and maintain procedures for conducting OSHMS management reviews
- Support the ESC in carrying out its responsibilities listed in bullets 2-4 below

AHJ

- Providing final interpretations of the NIST-adopted codes and standards relevant to fire, electrical, and life safety on all NIST-owned sites
 - Enforcing conformance to the adopted codes and standards on all NIST-owned sites
 - Enforcing industry best practices when the adopted codes and standards do not address specific issues

- Enforcing the more stringent requirement(s) when the adopted codes and standards conflict
- Ordering the correction of any deficiencies related to fire, electrical, and life safety and ensuring that corrective actions have been properly implemented
- Approving alternative materials or methods provided that the proposed design, use, or operation meets the intent of the adopted codes and standards and that the same or a greater level of protection is present when compared against the prescriptive requirements
- Working with the OUs and the Office of Facilities and Property Management (OFPM) on all construction projects and renovations on NIST-owned sites that affect or could affect fire, electrical, and life safety

OSH Program Managers

- Develop, deploy, and maintain their assigned programs in accordance with the requirements of the OSH program development, deployment, and maintenance program
- Carry out responsibilities specific to their assigned programs
- Serve as the primary points of contact and subject matter experts for their assigned programs
- Ensure effective communication with management and staff on program-related issues

ESC

- Participate in the development, deployment, and maintenance of OSH programs in accordance with the requirements of the OSH program development, deployment, and maintenance program
- Support the NIST Director and Associate Directors in conducting management reviews
 - Identify to the NIST Director and Associate Directors opportunities for improvement and the need for possible changes to the OSHMS
- Establish and maintain OSH objectives and plans for achieving those objectives, taking into account the results of management reviews
- Review and revise OSH objectives and plans for achieving those objectives no less frequently than every two years, taking into account:
 - Compliance with regulatory and other requirements
 - OSH risks
 - Incident history
 - Technological options

- Financial, operational, and business requirements
- The views of relevant interested parties
- Provide a forum for sharing information pertinent to the OHSMS and for identifying and addressing issues warranting NIST-level attention
- Provide a venue for members to provide input and feedback on the plans, priorities, programs, and services of OSHE
- Advise the NIST Director and Associate Directors on safety-related issues warranting their attention
- Operate in accordance with the ESC charter

OU Directors

General

- Assist the NIST Director and Associate Directors in carrying out their responsibilities
- Implement the NIST OSHMS in their respective OUs
- Demonstrate their commitment to the continual improvement of OSH performance
- Ensure that the employees and covered associates in their OUs participate as appropriate in the development, deployment, and maintenance of NIST's OSH programs
- Ensure that their OUs work in partnership with OSHE to develop, implement, maintain, and continually improve the NIST OSHMS

OU Space

- Implement all OSH directives applicable to their OU space (e.g., directives concerning hazard signage, chemical labeling and storage)²
- Establish, implement, and maintain administrative, and, where feasible and permitted by OFPM, physical, access controls for their OU space as necessary to protect the safety and health of their OU employees, covered associates, and visitors and those of other OUs

Common Spaces in OU-Assigned Buildings

- Implement all OSH directives applicable to the common spaces in their OU-assigned buildings
- Designate, for each OU-assigned building, at least one OU employee to serve as the point of contact for OSH issues in the common spaces in that building

² OU Directors (and subordinate managers) could carry out this responsibility by assigning individual OU spaces to OU employees and delegating to those employees the authority to carry out this responsibility for their assigned spaces.

OU Activities

- Implement all OSH directives applicable to their OU activities, including those aspects that pertain to the potential impact of those activities on the safety and health of individuals outside the spaces in which those activities are conducted

Activities of One or More OUs in Another OU's Space

- Director of the OU that owns the space (OU1)
 - Ensure the establishment and communication of the requirements necessary to protect OU1 employees, covered associates, and visitors from the hazards associated with activities conducted by other OUs in the space
 - Ensure the establishment and communication of the requirements necessary to protect the employees, covered associates, and visitors of other OUs from the hazards associated with other activities conducted in the space
- Director of the OU that owns the activity (OU2)
 - Ensure that the requirements established by OU1 to protect OU2 employees, covered associates, and visitors from the hazards associated with other activities conducted in the space are adequate and met
 - Ensure that the requirements established by OU1 for the conduct of OU2 activities in the space are met

Implementation of Plans for Achieving OSH Objectives

- Implement the plans, as applicable to their respective OUs, established to achieve NIST's OSH objectives

Chief Facilities Management Officer (in addition to the responsibilities for other OU Directors)

- Implement all OSH directives applicable to NIST's facilities infrastructure and grounds
- Determine, for each building, based on the information in the NIST space management system, which of the OUs with full-time building occupants has the most OU space in that building

OU Directors (in addition to the responsibilities above of all OU Directors) **and Subordinate Managers and Supervisors**

- Conduct or participate in management observations in their OUs to:
 - Help prevent injuries, illnesses, and incidents by increasing dialogue with employees and covered associates on creating and maintaining a safe workplace
 - Observe employees' and covered associates' behavior without threat of punishment
 - Provide positive reinforcement of safe work behaviors

Managers and Supervisors (in addition to the responsibilities above of all Managers and Supervisors)

- Demonstrate their commitment to the continual improvement of OSH performance
- Ensure that employees and covered associates in their organizations:
 - Are involved in hazard identification, risk assessments, and the determination of controls, as appropriate
 - Take responsibility for aspects of OSH over which they have control, including adherence to all applicable OSH requirements

NIST Employees and Covered Associates

- Take personal responsibility for their own safety and the safety of others, and for making safety an integral core value and vital part of the NIST culture in accordance with NIST P 7100.00
- Comply with all applicable requirements of the OSHMS and any additional applicable requirements established by their OUs or other OUs
- Participate as appropriate in the development, deployment, implementation, maintenance, and continual improvement of the OSHMS

DELEGATIONS OF AUTHORITY

CSO

- Approve changes to this order;
- Approve OSH suborders; suborder-specific directives, including procedures, notices, and guidance; and any associated deployment tools and OU procedures necessary to implement this order
- Re-delegate to the Deputy CSO, subordinate line managers, and other OSHE employees the authorities necessary to carry out CSO responsibilities, provided that such delegations are not inconsistent with other OSH directives

AHJ

- Delegate to other qualified OSHE engineers the authority to carry out AHJ responsibilities
- Establish industry best practices through evaluation of techniques or methodologies employed by other federal agencies or research institutes, scientific literature or treatise, or other data or fact that provides a strong basis of opinion

OU Directors

- Establish and communicate OU-specific OSH requirements, beyond those of the NIST OSHMS, deemed necessary to carry out their responsibilities under this order
- Re-delegate to subordinate line managers and other OU staff members, including OU/division safety personnel, the authorities necessary to carry out OU Director responsibilities, provided that such assignments and delegations are not inconsistent with other OSH directives

Director, NIST Center for Neutron Research (NCNR)

- Control access to Building 235

DIRECTIVE OWNER

150 Chief Safety Officer

APPENDICES

A. Revision History

Appendix A.

Revision History

Revision No.	Issue Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	05/15/13	05/15/13	05/15/13	None – Initial document
1	04/02/15	04/02/15	04/02/15	<ul style="list-style-type: none">• Added definition of “Associate”• Made order applicable to “Associates”
2	8/2/16	8/2/16	8/2/16	<ul style="list-style-type: none">• Added definitions of “Covered Associate” and “Non-R&D Contractor”• Made suborder applicable to “Covered Associates”• Added definition, responsibilities, and authorities of “Authority Having Jurisdiction”

Safety Rights and Responsibilities

NIST S 7101.01

Document Approval Date: 05/09/2014

Effective Date: 06/25/2014

1. PURPOSE

The purpose of this suborder is to delineate the key safety rights of all NIST employees. Employees' understanding and exercising those rights, in the context of carrying out their safety responsibilities, is critical toward making occupational safety and health an integral core value and vital part of the NIST culture.

2. BACKGROUND

- a. This suborder delineates the key safety rights of all employees and the procedures required by 29 Code of Federal Regulation (CFR) 1960.46 to "assure that no employee is subject to restraint, interference, coercion, discrimination, or reprisal for filing a report of an unsafe or unhealthful working condition, or other participation in agency occupational safety and health program activities, or because of the exercise by such employee on behalf of himself or herself or others of any right afforded by section 19 of the Act (i.e., the Occupational Safety and Health Act of 1970), Executive Order 12196, or this part (i.e., 29 CFR 1960)."¹
- b. In addition to having the safety rights delineated herein, employees also have the safety responsibilities delineated in [NIST O 710](#), Occupational Safety and Health Management System (see Section 9 of this suborder).

3. APPLICABILITY

The provisions of this suborder apply to all NIST employees.

¹ For an overview of rights afforded by the Occupational Safety and Health Act of 1970, see Occupational Safety and Health Administration [Publication 3021-09R 2011](#), Workers' Rights.

4. REFERENCES

- a. [Occupational Safety and Health Act of 1970, Section 19](#), Federal Agency Safety Programs and Responsibilities;
- b. [Executive Order 12196](#), Occupational Safety and Health Programs for Federal Employees;
- c. [29 CFR 1960](#), Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters
- d. [29 CFR 1960.28](#), Employee Reports of Unsafe or Unhealthful Working Conditions; and
- e. 29 CFR 1960, Subpart G, Allegations of Reprisal
 - (1) [29 CFR 1960.46](#), Agency Responsibility;
 - (2) [29 CFR 1960.47](#), Results of Investigations;
- f. [29 CFR 1977](#), Discrimination against Employees Under the Occupational Safety and Health Act of 1970;
 - (1) [29 CFR 1977.12](#), Exercise of Any Right Afforded by the Act;
- g. [NIST O 710](#), Occupational Safety and Health Management System (OSHMS); and
- h. [NIST P 710](#), Occupational Safety and Health.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. Employee Reporting of Unsafe or Unhealthful Working Conditions (UWCs);
- b. Personal Protective Equipment (PPE); and
- c. Safety Education and Training.

6. SAFETY RIGHTS

- a. General
 - (1) All NIST employees are entitled to a workplace free from recognized hazards causing or likely to cause death or serious physical harm.

b. Specific

To help assure a safe and healthful workplace, all NIST employees have the following rights:

- (1) To receive information on the NIST safety requirements and Occupational Safety and Health Administration (OSHA) standards applicable to their jobs.
- (2) To comply with, and obtain the benefits of, OSHA standards and other requirements applicable to their own actions or conduct.²
- (3) To receive information and training about the hazards to which they could be exposed in carrying out their assigned duties and methods to prevent harm.
- (4) To receive in a timely manner copies of the results of testing and monitoring done to identify and assess hazards in their work areas.
- (5) To observe the monitoring and measuring of toxic substances to which they could be exposed and to have access to any records of their exposure.
- (6) To obtain copies of their NIST medical records.
- (7) To obtain copies of OSHA-required workplace injury and illness records, i.e., NIST's OSHA Form 300 log.
- (8) To communicate orally or in writing with their supervisors or managers about occupational safety or health matters, e.g., to ask questions, express safety concerns, report work-related injuries or illnesses, or request safety data sheets and other information to which they are entitled.
- (9) To refuse to perform an assigned task when they:³
 - (a) Have a reasonable belief that performing the task would subject them to death or serious injury;⁴
 - (b) Refuse in good faith (i.e., genuinely believe that such a danger exists);
 - (c) Have requested that their supervisors or managers eliminate the danger but they have failed to do so; and

² For example, employees have the right to employer-provided PPE required by OSHA standards (see the PPE suborder) and to engage in work practices required by OSHA standards.

³ See 29 CFR 1977.12(b).

⁴ A "reasonable belief" is a belief with which a reasonable person would agree.

- 114 (d) Have a reasonable belief, due to the urgency of the danger, that there is insufficient
115 time to eliminate it through other channels, such as requesting an inspection by
116 Office of Safety, Health, and Environment (OSHE) or OSHA.
117
- 118 (10) To report UWCs to the Chief Safety Officer (CSO) or OSHA to request inspections by
119 OSHE or OSHA, respectively.⁵
120
- 121 (a) In reporting UWCs to the CSO, to have their names not disclosed to anyone outside
122 of OSHE other than an Authorized Representative of the Secretary of Labor, or as
123 otherwise required by law.
124
- 125 (b) In reporting UWCs to OSHA, to have their names not disclosed to anyone other than
126 an Authorized Representative of the Secretary of Labor, or as otherwise required by
127 law.
128
- 129 (c) Before reporting UWCs to the CSO, employees should, whenever possible, abate the
130 dangers themselves or work with their management to abate the dangers, as this will
131 generally result in prompt abatement of UWCs.
132
- 133 (d) Before reporting UWCs to OSHA, employees should, whenever possible, abate the
134 dangers themselves, work with their management to abate the dangers, or report the
135 dangers to the CSO to request inspections by OSHE, as this will generally result in
136 prompt abatement of UWCs.
137
- 138 (11) To exercise their safety rights without restraint, interference, coercion, discrimination, or
139 reprisal.
140
- 141 (12) To file a grievance in accordance with the appropriate procedure (i.e., administrative or
142 negotiated) or to file a complaint with the Office of the Special Counsel if they believe
143 they have been subject to restraint, interference, coercion, discrimination, or reprisal.^{6, 7}
144
145

⁵ The Employee Reporting of UWCs suborder provides NIST's procedures for employee reporting of UWCs to the CSO. It also provides guidance to employees and management on responding to UWCs through direct employee and management action prior to reporting UWCs to the CSO or OSHA.

⁶ Protection from discrimination in this context means that an employer cannot retaliate by taking "adverse action" against workers, such as firing or laying off; blacklisting; demoting; denying overtime or promotion; disciplining; denying benefits; failing to hire or rehire; intimidation; making threats; reassignment affecting prospects for promotion; or reducing pay or hours. See [OSHA Publication 3021-09R 2011](#). The protections take the form of administrative or whistleblower protections as opposed to civil-rights protections.

⁷ Contact the Office of Human Resources Management to file a grievance; call 1-800-872-9855 to file a complaint with the Office of Special Counsel.

146 **7. DEFINITIONS**

- 147 a. Authorized Representative of the Secretary of Labor – A person or agent of the Secretary of
148 Labor whose authority and jurisdiction originates from the Secretary of Labor; routinely a
149 Department of Labor employee.
150
151 b. UWC – Any condition or practice in any work area that an employee believes may have a
152 direct or immediate impact on safety or health.
153

154
155 **8. ACRONYMS**

- 156 a. CFR – Code of Federal Regulations
157
158 b. CSO – Chief Safety Officer
159
160 c. O – Order
161
162 d. OSHA – Occupational Safety and Health Administration
163
164 e. OSHE – Office of Safety, Health, and Environment
165
166 f. OSHMS – Occupational Safety and Health Management System
167
168 g. P – Policy
169
170 h. PPE – Personal Protective Equipment
171
172 i. UWC – Unsafe or Unhealthful Working Condition
173
174

175 **9. ROLES AND RESPONSIBILITIES**

- 176 a. NIST Employees (from [NIST O 710](#)):
177
178 (1) Take personal responsibility for their own safety and the safety of others, and for making
179 safety an integral core value and vital part of the NIST culture in accordance with [NIST P](#)
180 [710](#);
181
182 (2) Comply with all applicable requirements of the OSHMS and any additional applicable
183 requirements established by their OUs or other OUs; and
184

- (3) Participate as appropriate in the development, deployment, implementation, maintenance, and continual improvement of the OSHMS.

b. NIST Line Management:

- (1) Provide employees with a workplace that is free from recognized hazards causing or likely to cause death or serious physical harm;

- (2) Ensure that employee safety rights are fulfilled;

- (3) Maintain a work environment in which employees feel free to exercise their safety rights without fear of restraint, interference, coercion, discrimination, or reprisal;

- (4) Address via appropriate disciplinary and other avenues instances where it has been determined that employees have been subjected to restraint, interference, coercion, discrimination, or reprisal for exercising their safety rights.

c. CSO:

- (1) Ensure that OSHE staff members do not disclose the names of reporting employees who desire to remain anonymous to anyone outside of OSHE other than an Authorized Representative of the Secretary of Labor, or as otherwise required by law; and

- (2) Ensure that information on employees' safety rights is included in the NIST General Safety Training and in the training for line managers, safety and health specialists, and OU/division safety personnel required by the Safety Education and Training suborder.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

11. DIRECTIVE OWNER

CSO

12. APPENDICES

None

3 **Employee Reporting of Unsafe or** 4 **Unhealthful Working Conditions**

5
6
7 NIST S 7101.02

8 Document Approval Date: 10/02/2014

9 Effective Date: 04/01/2015
10
11

12 **1. PURPOSE**

- 13 a. The purpose of this suborder is to establish a formal mechanism to assure prompt analysis
14 and response to employee reports of perceived unsafe or unhealthful working conditions
15 (UWCs), i.e., of conditions or practices, in any NIST workplace, that an employee believes
16 may have a direct or immediate impact on safety or health. The formal mechanism
17 comprises:

- 18
19 (1) Employee reporting of perceived UWCs to the Chief Safety Officer (CSO);
20
21 (2) Inspections of reported UWCs by the Office of Safety, Health, and Environment (OSHE);
22
23 (3) The identification and implementation of corrective actions by the responsible
24 Organizational Units (OUs), as necessary; and
25
26 (4) Notifications to OSHE and the reporting employees when corrective actions have been
27 completed.
28

- 29 b. This suborder also outlines the process by which employees and management should abate
30 perceived UWCs through direct employee or management action. **Before reporting UWCs**
31 **to the CSO, employees should, whenever possible, abate the UWCs themselves or work**
32 **with their management, OU/division safety personnel, OSHE, or others to abate the**
33 **UWCs, as this will generally result in prompt analysis and abatement of UWCs.** See
34 Section 9a and Appendix A, Flow Chart for Employee/Management Actions in Response to
35 Perceived UWCs.
36
37
38

2. BACKGROUND

- a. [NIST P 710](#) articulates NIST's commitment to make occupational safety and health an integral core value and vital part of the NIST culture by, in part, fostering a work environment in which employees are encouraged to report and raise safety and health issues without fear of reprisal.
- b. NIST must meet the requirements of 29 Code of Federal Regulations (CFR) 1960.28, Employee Reports of Unsafe or Unhealthful Working Conditions, which states that employees have the right and are encouraged to report UWCs to an agency safety and health official to request inspections of those conditions.¹ Implementation of this suborder through the requirements in Section 6 and the roles and responsibilities in Section 9 fulfills those requirements.
- a. NIST must meet the requirements of 29 CFR 1960.26, Conduct of Inspections, and 29 CFR 1960.30, Abatement of Unsafe or Unhealthful Working Conditions, which establish minimum UWC inspection and abatement requirements. Implementation of this suborder through the requirements in Section 6 and the roles and responsibilities in Section 9 fulfills those requirements.

3. APPLICABILITY

- a. The requirements in Section 6 of this suborder apply to UWCs reported by employees to the CSO to request inspections of those UWCs by OSHE.
- b. The process outlined in Appendix A of this suborder applies to perceived UWCs that can be addressed by employees themselves or by employees working with their line management, OU/division safety personnel, OSHE, or others,² This process should be followed whenever possible, but its existence does not preclude employees from reporting UWCs to the CSO at any point to request inspections by OSHE.

4. REFERENCES

For references common to all NIST Occupational Safety and Health (OSH) suborders, see [NIST O 710](#). References specific or pertinent to this suborder are:

- a. [NIST P 710](#), Occupational Safety and Health Policy

¹ For NIST, the agency safety and health official is the CSO, who is also the Director of OSHE.

² This suborder distinguishes between employees communicating UWCs to OSHE to request safety assistance and employees reporting UWCs to the CSO to request inspections by OSHE. OSHE will ascertain employee intent when it receives employee requests.

- b. [OSH Act of 1970, Section 19](#), Federal Agency Safety Programs and Responsibilities;
- c. [Executive Order 12196](#), Occupational Safety and Health Programs for Federal Employees;
- d. [29 CFR 1960.28](#), Employee Reports of Unsafe or Unhealthful Working Conditions;
- e. [29 CFR 1960.26](#), Conduct of Inspections; and
- f. [29 CFR 1960.30](#), Abatement of Unsafe or Unhealthful Working Conditions.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

Other NIST occupational safety and health suborders applicable to work covered by this suborder include:

- a. Safety Rights and Responsibilities;
- b. Stop Work;
- c. Safety Education and Training; and
- d. Incident Reporting and Investigation.

6. REQUIREMENTS

As indicated in Section 1, employees should, whenever possible, abate UWCs themselves or work with their management, OU/division safety personnel, OSHE, or others to abate the UWCs before reporting them to the CSO to request inspections by OSHE. The present section delineates the requirements of the formal mechanism for reporting UWCs to the CSO, and Section 9 provides the associated responsibilities. Appendix B, Employee Reporting of UWCs to the CSO, presents most of this information in flow chart.

a. Reporting of Perceived UWCs to the CSO to Request Inspections by OSHE

(1) Such perceived UWCs should be reported by employees to the CSO using the most expeditious means available.³

(2) If it is determined by OSHE that there are not reasonable grounds to believe that a reported UWC exists and that OSHE does not plan to conduct an inspection based on

³ For example, reports of perceived UWCs may be made by calling x5375, Option 3.

such report, the reporting employee shall be notified by the CSO of that determination in writing within 15 calendar days of receipt of the report.

b. Inspection of Reported UWCs by OSHE

(1) Reported UWCs shall be characterized immediately by OSHE as imminent danger, serious, or other than serious.⁴

(2) If an imminent-danger UWC is suspected by OSHE based on the information reported, a responsible line manager in the responsible OU will be notified immediately by OSHE, with instructions to remove employees from the danger as quickly as possible.⁵

(3) Reported UWCs shall be inspected by OSHE within the following timeframes:

(a) As soon as possible for suspected imminent-danger UWCs but always within 24 hours;

(b) 3 business days for suspected serious UWCs; and

(c) 20 business days for suspected other-than-serious UWCs;

(4) Inspected UWCs shall be characterized by OSHE as imminent danger, serious, or other than serious using the procedure provided in Appendix C.

(5) If an imminent-danger UWC is identified during an inspection, an oral stop-work Order shall be issued by the OSHE inspector(s) in accordance with the requirements of the Stop Work suborder.⁶

(6) A written inspection report that includes a description of the inspection procedures and details any findings and recommended corrective actions shall be prepared by OSHE for each reported UWC.

⁴ Technically, imminent-danger conditions are a subset of serious conditions. Nevertheless, serious conditions that present an imminent danger are referred to simply as “imminent danger conditions”, and serious conditions that do not present an imminent danger are referred to as “serious conditions”.

⁵ OSHE will attempt to contact the Group Leader first, followed by the Division Chief.

⁶ The issuance of an oral stop-work order starts a separate process that proceeds in parallel with the inspection process; that is, the stop-work process does not replace or supersede the inspection process. An oral stop-work order requires specific actions to be taken by the OU Director, CSO, and others. Refer to the Stop Work suborder for details.

c. Notices of UWCs

- (1) If an inspection results in a finding of an imminent-danger or serious UWC, a written notice of an UWC shall be issued by OSHE to the responsible Division Chief and provided to the reporting employee along with the inspection report.
- (2) The UWC notice shall characterize and describe the nature of the UWC, indicate any regulations or other requirements it violates, and provide a timeframe for abatement.
- (3) The UWC notice, or a copy of it, shall be posted immediately by the OU, either at or near the location where the UWC exists or existed; if that is not possible, it shall be posted in a prominent place where all affected employees can read it.
- (4) Any additional notices describing special measures in effect during abatement of the UWC shall also be posted by the OU.
- (5) Each notice, or a copy of it, shall remain posted until it has been determined by the OU that the UWC has been abated or for 3 business days, whichever is longer.

d. Abatement of UWCs

- (1) Upon receipt by an OU of an inspection report confirming the existence of an UWC, corrective actions shall be identified and implemented by the OU.
- (2) If it is determined by the OU that the corrective actions for imminent-danger or serious UWCs cannot be completed within 30 calendar days of receipt of the inspection report, a corrective-action plan (CAP), including any interim measures necessary to protect employees, shall be developed and provided to OSHE by the OU before 30 calendar days have elapsed and by the means specified in the inspection report.
- (3) Corrective actions for imminent-danger and serious UWCs shall be developed and implemented by the OU within the timeframe specified in the associated UWC notice. If this is not possible, a written request for an extension shall be submitted to OSHE by the responsible Division Chief before the end of the timeframe specified in the notice and by the means specified in the inspection report.

e. Communication

- (1) Inspection reports shall be provided by OSHE to reporting employees and responsible Division Chiefs within 15 calendar days of UWCs being inspected, unless there are

compelling reasons why such reports cannot be provided within 15 calendar days, in which case reporting employees and responsible Division Chiefs shall be informed of the delay.

(2) When the corrective actions for abating UWCs have been completed, the corrective actions and their completion dates shall be provided to OSHE by the responsible Division Chief by the means specified in the inspection report.

(3) When the corrective actions for abating UWCs have been completed by the OUs, the corrective actions and their completion dates shall be provided to reporting employees by OSHE.

7. DEFINITIONS

For definitions common to all NIST OSH suborders, see [NIST O 710](#). Definitions specific to this suborder are as follows:

- a. Authorized Representative of the Secretary of Labor – A person or agent of the Secretary of Labor whose authority and jurisdiction originates from the Secretary of Labor; routinely a Department of Labor employee.
- b. Corrective-Action Plan (CAP) – A set of planned actions to abate a recognized deficiency and their estimated completion dates.
- c. Imminent Danger (Condition or Practice) – Any serious condition or practice in any workplace which is such that a danger exists which could reasonably be expected to cause death or serious physical harm immediately or before the imminence of such danger can be eliminated through normal procedures.
- d. Serious (Condition or Practice) – A condition or practice in any workplace such that there is a substantial probability that death or serious physical harm could result.
- e. UWC – Any condition or practice in any workplace that could have a direct or immediate adverse impact on safety or health.⁷
- f. Workplace – A physical location where NIST work is performed.

⁷ Note that UWCs are conditions or practices, not “events”. As such, UWCs are not “incidents” as defined in the Incident Reporting and Investigation suborder, i.e., they are not work-related **events** in which any of the following, individually or in combination, occurred or could have occurred: an injury or illness; an unauthorized spill or release of hazardous or regulated material to the environment; damage or loss of equipment or property, and they are not reported in the NIST Incident Reporting and Investigation System (IRIS).

8. ACRONYMS

For acronyms common to all NIST OSH suborders, see [NIST O 710](#). Acronyms specific or pertinent to this suborder are:

- a. CAP – Corrective-Action Plan
- b. CFR – Code of Federal Regulations
- c. CSO – Chief Safety Officer
- d. OSH – Occupational Safety and Health
- e. OSHE – Office of Safety, Health, and Environment
- f. OU – Organizational Unit
- g. UWC – Unsafe or Unhealthful Working Condition

9. ROLES AND RESPONSIBILITIES

For roles and responsibilities applicable to all NIST OSH programs, see [NIST O 710](#). Roles and responsibilities specific to this suborder are as follows:

a. All Employees:

- (1) Before reporting perceived UWCs to the CSO to request inspections by OSHE, follow the process outlined in Appendix A for abating perceived UWCs; and
- (2) When reporting UWCs to the CSO to request inspections by OSHE, indicate whether they desire that their names not be disclosed to anyone outside of OSHE other than an Authorized Representative of the Secretary of Labor, or as otherwise required by law.

b. OU Line Management and OU/Division Safety Personnel:

- (1) Upon receiving employee communications of UWCs, follow the process outlined in Appendix A for responding to the UWCs.

c. Division Chiefs:

- (1) Upon receiving UWC notices from OSHE, ensure that those notices are posted in accordance with the requirements in Sections 6c(3)-(5);
- (2) Upon receiving inspection reports from OSHE for UWCs in their respective divisions, ensure that those UWCs are abated in accordance with the requirements in Section 6d; and
- (3) When the corrective actions for abating UWCs have been completed, provide those corrective actions and their completion dates to OSHE by the means specified in the inspection report.

d. CSO:

- (1) Ensure that OSHE staff members receiving employee communications regarding perceived UWCs determine whether employees are requesting safety assistance or reporting UWCs to the CSO to request inspections by OSHE;⁸
- (2) Ensure that OSHE staff members do not disclose the names of reporting employees who desire non-disclosure to anyone outside of OSHE other than an Authorized Representative of the Secretary of Labor, or as otherwise required by law;
- (3) Ensure that employee oral reports of perceived UWCs to the CSO are reduced to writing and contain the following information:
 - (a) Name and contact information of the reporting employee;
 - (b) Indication of whether the reporting employee desires that his or her name not be disclosed to anyone outside of OSHE other than an Authorized Representative of the Secretary of Labor, or as otherwise required by law;
 - (c) Brief description of the UWC;
 - (d) Date and time the UWC was first observed;
 - (e) Where the UWC is located, *e.g.*, site, building, room, *etc.*;

⁸ If it is determined that employees are requesting safety assistance, OSHE will assist those employees in promptly analyzing and abating the perceived UWCs. As indicated in Section 3b, the provision of such assistance is outside the scope of this suborder.

- 302 (f) OU responsible for the space where the UWC is located, if known; and
303
- 304 (g) Brief description of any immediate measures taken to abate the UWC and to notify
305 potentially affected employees;
306
- 307 (4) If it is determined by OSHE that there are not reasonable grounds to believe that a
308 reported UWC exists and that OSHE does not plan to conduct an inspection based on
309 such report, ensure that the reporting employee is notified of that determination in
310 writing within 15 calendar days of receipt of the report;
311
- 312 (5) Ensure that all other reported UWCs are characterized immediately as imminent danger,
313 serious, or other than serious and inspected by OSHE in accordance with the
314 requirements in Sections 6b(3)-(6);
315
- 316 (6) If an imminent-danger UWC is suspected based on reported information, ensure that the
317 responsible supervisor or other official in the responsible OU is notified immediately to
318 remove employees from the danger as quickly as possible;
319
- 320 (7) Ensure that inspection reports are provided to reporting employees and responsible
321 Division Chiefs within 15 calendar days of UWCs being inspected, or if there are
322 compelling reasons why such reports cannot be provided within 15 calendar days, that
323 reporting employees and responsible Division Chiefs are informed of the delay;
324
- 325 (8) When an inspection results in a finding of an imminent-danger or serious UWC, ensure
326 that a written notice is issued in accordance with the requirements of Sections 6c(1)-(2);
327
- 328 (9) When corrective actions for abating UWCs have been completed by the OUs, ensure
329 that the reporting employee is provided with those corrective actions and their
330 completion dates;
331
- 332 (10) For each reported UWC, ensure that a sequentially numbered case file, coded for
333 identification and containing the following information, is maintained and retained for a
334 minimum of five years after abatement:
335
- 336 (a) The information listed in Section 9d(3);
337
- 338 (b) Documentation of OSHE's determination that there are not reasonable grounds to
339 believe that a reported UWC exists and of its decision not to conduct an inspection
340 based on such report, when applicable;
341

- 342 (c) OSHE's initial characterization of all other UWCs as imminent danger, serious, or
343 other than serious;
344
- 345 (d) OSHE's final characterization of the UWC, if different from the initial
346 characterization;
347
- 348 (e) The names of the OSHE staff member(s) who conducted the inspection;
349
- 350 (f) A copy of the inspection report;
351
- 352 (g) Copies of any UWC notices issued by OSHE and any additional notices posted by
353 the OU;
354
- 355 (h) A copy of the CAP developed by the OU when it has been determined by the OU
356 that corrective actions cannot be completed within 30 calendar days of receipt of the
357 inspection report; and
358
- 359 (i) The corrective actions taken by the OU to abate the UWC and their completion
360 dates;
361
- 362 (11) Ensure that training on this suborder is included in the training for line managers, safety
363 and health specialists, and OU/division safety personnel required by the Safety
364 Education and Training suborder; and
365
- 366 (12) Ensure that case files of employee-reported UWCs are made available to the Secretary
367 of Labor or the Secretary's authorized representative upon request.
368
369

370 **10. AUTHORITIES**

371 For authorities applicable to all NIST OSH suborders, see [NIST O 710](#). In addition:

373 a. Employees:

- 374
- 375 (1) Report UWCs directly to an authorized representative of the Secretary of Labor.^{9, 10}
376
377

⁹ The Secretary of Labor encourages employees to use agency procedures as the most expeditious means of achieving abatement of UWCs.

¹⁰ UWCs may be reported to an authorized representative of the Secretary of Labor by calling 1-800-321-OSHA.

378 **11. DIRECTIVE OWNER**

379 CSO

380

381

382 **12. APPENDICES**

383 A. Flow Chart for Employee/Management Actions in Response to Perceived UWCs

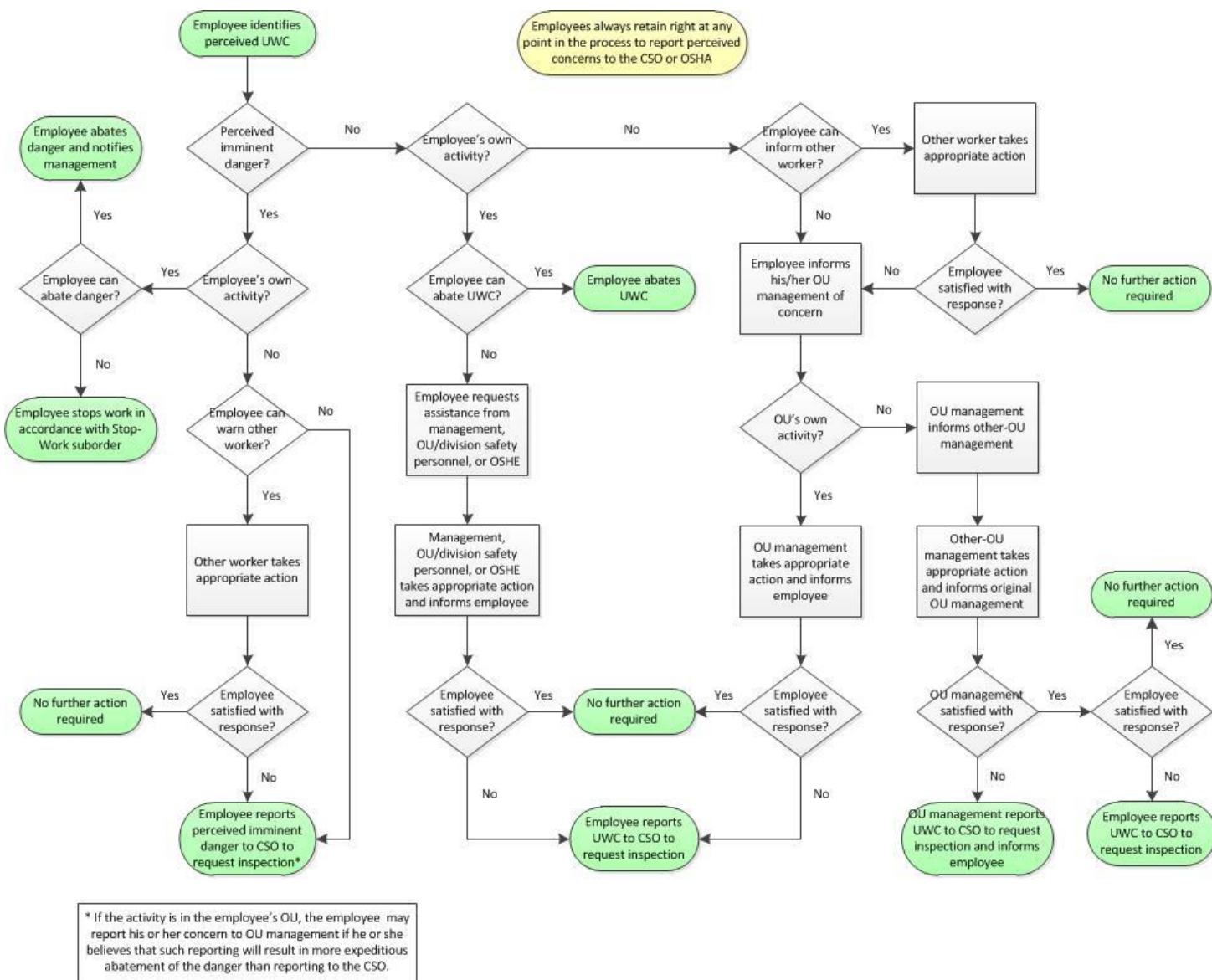
384

385 B. Flow Chart for Employee Reporting of UWCs to the CSO

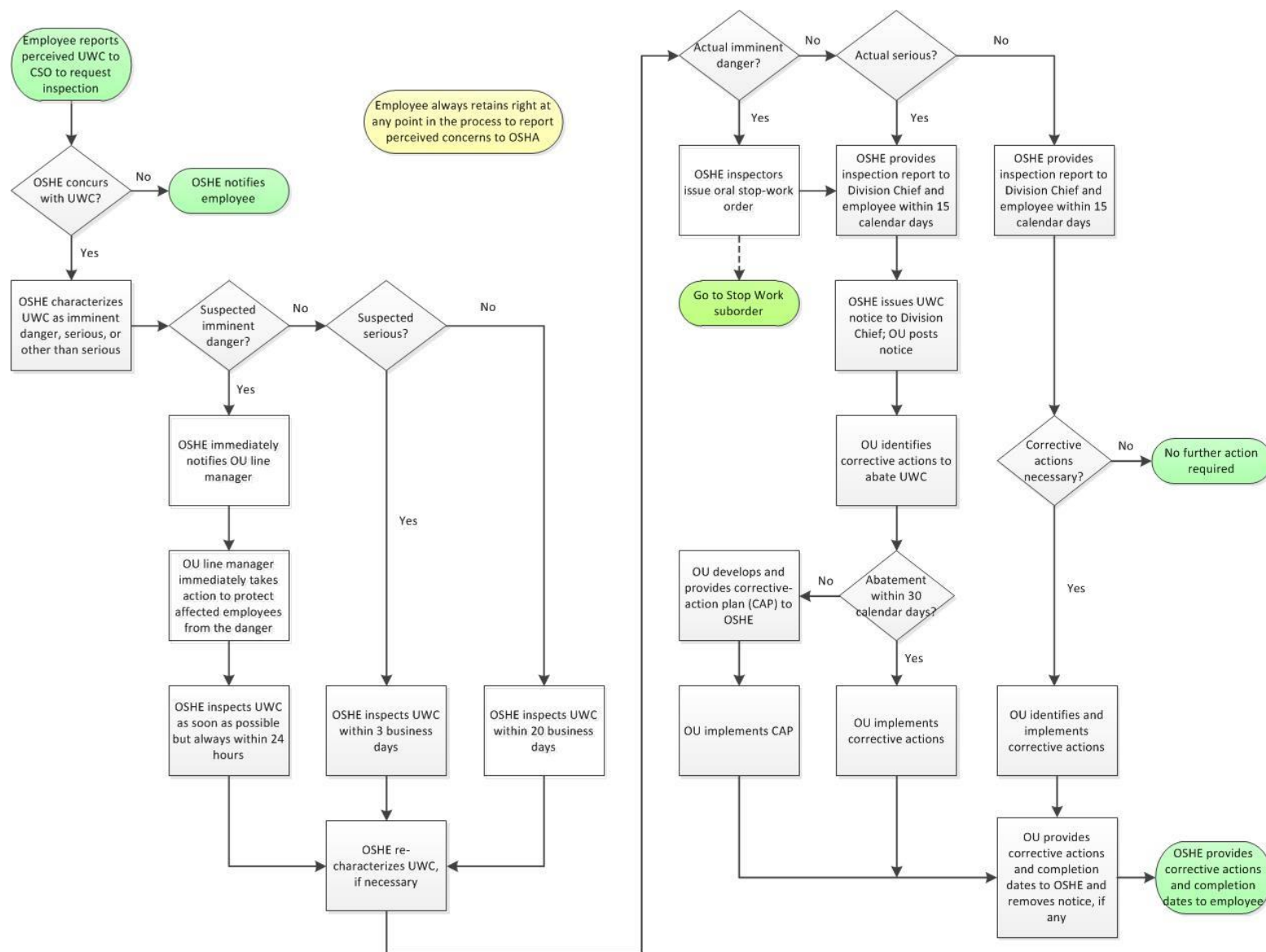
386

387 C. Serious and Imminent Danger Determinations by OSHE

Appendix A. Flow Chart for Employee/Management Actions in Response to Perceived UWCs



Appendix B. Flow Chart for Employee Reporting of UWCs to the CSO



Appendix C. Serious and Imminent Danger Determinations by OSHE

A Notice of Unsafe or Unhealthful Working Conditions (Notice) is required when a workplace inspection identifies a situation that meets the definition of a serious working condition. In addition, a serious condition that poses an imminent danger requires issuance of a Stop Work Order, except when it is immediately corrected and controls are in place to make its recurrence unlikely. This appendix outlines the procedure that shall be followed by OSHE inspectors for making serious working condition and imminent danger determinations.

Determination of a “Serious” Condition.

A serious working condition is one where a safety deficiency presents a hazard to one or more persons in which there is a substantial probability that death or serious physical harm could result. Inspectors and investigators will consider whether there is a substantial probability¹¹ that death or serious physical harm could result from an incident or exposure relating to the safety deficiency using the following three step process:

Step 1. Identify the type of potential hazards that the safety deficiency presents. If the deficiency presents more than one type of hazard, the inspector/investigator will determine which hazard could reasonably be predicted to result in the most severe injury or illness and will use that as the basis for the determination.

The following examples illustrate this step:

Example A: Employees are observed working at the unguarded edge of an open-sided floor 30 feet above the ground. The type of hazard is a fall from the edge of the floor to the ground below.

Example B: Employees are observed working in an area in which debris is located. The type of hazard is tripping on debris.

Example C: Employees are observed working with methylene chloride without ventilation or respiratory protection. The type of hazard is inhalation exposure to methylene chloride.

Step 2. Identify the most serious injury or illness that could reasonably be expected to result from the potential hazardous exposure identified in Step 1. In making this determination,

¹¹ NOTE: The key determination is the likelihood that death or serious harm will result **IF** an accident or exposure occurs. **The likelihood of an accident occurring is not addressed in making this determination.**

inspectors/investigators shall consider all factors that would affect the severity of the injury or illness that could reasonably result from the exposure to the hazard.

For conditions involving exposure to air contaminants or harmful physical agents, inspectors/investigators will consider the concentration levels of the contaminant or physical agent in determining the types of illness that could reasonably result from the exposure. Inspectors/investigators will also consider the nature of the operation from which the exposure results, such as:

- Whether the exposure is regular and ongoing or is of limited frequency and duration;
- How long employees have worked at the operation in the past;
- Whether employees are performing functions which can be expected to continue; and
- Whether work practices, engineering controls, production levels, and other operating parameters are typical of normal operations.

The following examples align with the previous examples to illustrate this step:

Example A: If an employee falls from the edge of an open-sided floor 30 feet to the ground below, the employee could die, break bones, suffer a concussion, or experience other serious injuries that would substantially impair a body function.

Example B: If an employee trips on debris, the trip may cause abrasions or bruises, but it is only marginally predictable that the employee could suffer a substantial impairment of a bodily function. If, however, the area is littered with protruding rebar, broken glass, or other sharp objects, it is reasonably predictable that an employee who tripped on debris could suffer deep cuts/punctures which could require suturing.

Example C: If an employee is exposed regularly to methylene chloride at 100 ppm, it is reasonable to predict that cancer could result.

Step 3. Determine whether the type of injury or illness identified in Step 2 could include death or a form of serious physical harm. In making this determination, utilize the following definition of serious physical harm: Impairment of the body in which part of the body is made functionally useless or is substantially reduced in efficiency on or off the job. Such impairment may be permanent or temporary, chronic or acute. Injuries involving such impairment would usually require treatment by a medical doctor or other licensed health care professional.

Injuries that constitute serious physical harm include, but are not limited, to:

- Amputations (loss of all or part of a bodily appendage);
- Concussion;

- Crushing (internal, even though skin surface may be intact);
- Fractures (simple or compound);
- Burns or scalds, including electric and chemical burns;
- Cuts, lacerations, or punctures involving significant bleeding and/or requiring suturing;
- Sprains and strains; and
- Musculoskeletal disorders.

Illnesses that constitute serious physical harm include, but are not limited, to:

- Cancer;
- Respiratory illnesses (silicosis, asbestosis, byssinosis, etc.);
- Hearing impairment;
- Central nervous system impairment;
- Visual impairment; and
- Poisoning.

The following examples align with the previous examples to illustrate this step:

Example A: If an employee falls from the edge of an open-sided floor 30 feet to the ground below, the likely result (i.e. death, broken bones, a concussion, or other serious injuries that would substantially impair a body function) would support a “serious” determination.

Example B: If an employee trips on debris in an area without other hazards (e.g. impalement) where it is unlikely that the employee could suffer a substantial impairment, a determination of “other than serious” would be warranted. If, however, the area is littered with protruding rebar, broken glass, or other sharp objects that would likely cause deep cuts/punctures which could require suturing, a determination of “serious” would be more appropriate.

Example C: Routine exposure to methylene chloride at levels that could reasonably result in cancer would support a “serious” determination.

Determination of an “Imminent Danger” Condition.

An imminent danger is one where a safety deficiency presents a hazard which could reasonably be expected to cause death or serious physical harm immediately or before the imminence of such danger can be eliminated through normal procedures.

When making an imminent danger determination, inspectors and investigators will consider whether the following conditions are present:

- The deficiency constitutes a serious¹² condition as outlined above; **and**
- It is reasonably likely that a serious incident could occur immediately or, if not immediately, then before abatement would otherwise be implemented.

This determination is highly dependent upon the specific activities, co-located hazards, work practices, and other factors present in the work environment.

¹² For a health hazard, exposure to the toxic substance or other hazard must cause harm to such a degree as to shorten life or be immediately dangerous to life and health (IDLH) or cause substantial reduction in physical or mental efficiency or health, even though the resulting harm may not manifest itself immediately.

Stop Work

NIST S 7101.03

Effective Date: 03/31/2015

Document Approval Date: 05/23/2014

1. PURPOSE

The purpose of this suborder is establish a formal mechanism to ensure employees are not exposed to workplace conditions or practices that present real danger of death or serious injury before the conditions can be corrected through regular channels.

2. BACKGROUND

- a. [NIST O 710](#) articulates NIST's expectation that all employees take personal responsibility for their own safety and the safety of their coworkers by:

- (1) Never working under unsafe conditions; and
- (2) Addressing or promptly reporting unsafe or unhealthful working conditions (UWCs).

This suborder supports employees in carrying out these personal responsibilities.

- b. The Safety Rights and Responsibilities suborder documents the right of all employees to refuse to perform an assigned task, i.e., stop their own work, when they:¹

- (1) Have a reasonable belief that performing the task would subject them to death or serious injury;²
- (2) Refuse in good faith (i.e., genuinely believe that such a danger exists);
- (3) Have requested that their supervisors or managers eliminate the danger but they have failed to do so; and

¹ See 29 CFR 1977.12(b).

² A "reasonable belief" is a belief with which a reasonable person would agree.

- (4) Have a reasonable belief, due to the urgency of the danger, that there is insufficient time to eliminate it through other channels, such as requesting an inspection by Office of Safety, Health, and Environment (OSHE) or Occupational Safety and Health Administration.

This suborder, in conjunction with the Employee Reporting of UWCs suborder, provides an avenue for employees to seek correction of dangerous conditions.

3. APPLICABILITY

- a. This suborder applies to all work activities performed by NIST employees.

4. REFERENCES

For references common to all NIST Occupational Safety and Health (OSH) suborders, see [NIST O 710](#). References specific or pertinent to this suborder are:

- a. [NIST P 710](#), Occupational Safety and Health Policy
- b. [OSH Act of 1970, Section 19](#), Federal Agency Safety Programs and Responsibilities;
- c. [Executive Order 12196](#), Occupational Safety and Health Programs for Federal Employees;
- d. [29 CFR 1960.28](#), Employee Reports of UWCs;
- e. [29 CFR 1960.26](#), Conduct of Inspections; and
- f. [29 CFR 1960.30](#), Abatement of UWCs.
- g. [29 CFR 1977.12](#), Exercise of Any Right Afforded by the Act;

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

Other NIST occupational safety and health suborders applicable to this suborder include:

- a. Safety Rights and Responsibilities;
- b. Employee Reporting of UWCs;
- c. Work and Worker Authorization Based on Hazard Reviews (“Hazard Review”); and

- d. Safety Education and Training.

6. REQUIREMENTS

Appendix A presents a high-level schematic of Sections 6a-c.

a. Employee-Initiated Stop Work of their Assigned Activity

- (1) An employee shall stop work on their assigned activity if they believe in good faith (i.e., a reasonable person would agree) that they are exposed to imminent-danger conditions or practices and they are unable to abate the danger immediately.³
- (2) As part of stopping work, the employee shall:
 - (a) Discontinue the hazardous activity;
 - (b) Inform co-workers exposed to the hazard to discontinue the hazardous activity;
 - (c) Separate any other affected workers from the hazard;
 - (d) Maintain a safe distance from the hazard;
 - (e) Initiate administrative controls, such as temporary warning signs, tape, or cones to prevent exposure to the hazard and inadvertent re-start of the activity; and
 - (f) Notify the line manager responsible for the work activity.
- (3) Before the work activity is re-started, the responsible line manager shall evaluate the concern that triggered the decision to stop work.⁴
- (4) If the responsible line manager determines that the concern is valid (i.e., an imminent danger exists), he or she shall initiate the following actions before the work activity can be re-started:
 - (a) If work and workers have not been authorized based on an approved hazard review, ensure that a hazard review addressing the danger is conducted and approved and that work and workers are authorized in accordance with the requirements of the Hazard Review suborder; or

³ Terms are defined in Section 7, Definitions.

⁴ If requested, OSHE will provide technical support to evaluate the concern.

- (b) If work and workers have been authorized based on an approved hazard review, ensure that the hazard review is re-reviewed, revised, and reapproved as necessary to address the danger and that work and workers are re-authorized, all in accordance with the requirements of the Hazard Review suborder.
 - (5) If the responsible line manager determines that an imminent danger does not exist, he or she shall inform the affected employees of the basis for that conclusion and direct employees to re-start the work activity.
 - (6) An employee who disagrees with the responsible line manager's determination and believes that re-starting work will result in exposure to an imminent danger shall report their concern immediately to the CSO to request an inspection by OSHE in accordance with the requirements of the UWCs suborder.⁵
- b. Employee-Initiated Stop Work of an Assigned Activity Performed by Other Workers
- (1) An employee observing other workers (e.g., different project, different OU) exposed to working conditions that he or she believes present an imminent danger shall, whenever possible:
 - (a) Warn the other worker(s) of the danger in a manner that does not increase the danger; and
 - (b) Urge the other workers to stop work in accordance with the requirements in Section 6a(2).
 - (2) If it is not possible to warn the other worker(s) of the danger immediately, or the other worker(s) does not stop work when the employee continues to believe that an imminent danger exists, the employee shall immediately report his or her concern to the CSO to request an inspection by OSHE in accordance with the requirements of the UWCs suborder.
 - (a) If the activity believed to present an imminent danger is in the employee's OU, the employee may report his or her concern to OU management if he or she believes that such reporting will result in more expeditious abatement of the danger than reporting to the CSO.

⁵ Employees should report their concerns to the CSO to request inspections by OSHE using the most expeditious means available, e.g., by calling x 5375, Option 3 and requesting an inspection.

c. OSHE-Initiated Stop Work

- (1) An OSHE staff member shall issue an oral stop-work order (SWO) when, through inspection or other evaluation, he or she identifies a working condition or practice that presents an imminent danger to one or more persons at any NIST workplace.⁶
- (2) When conditions warrant the issuance of an oral SWO, the OSHE staff member shall immediately:
 - (a) Instruct affected employees to stop work in a manner that does not increase the danger;
 - (b) Provide interim instructions to secure the work activity (e.g., using signage or barriers) to prevent exposure to the danger and inadvertent restart of the activity; and
 - (c) Inform the responsible line manager and OU Director and the CSO of issuance of the oral SWO.
- (3) As soon as possible, the CSO will evaluate the need for the continuance of the oral SWO and either:
 - (a) Notify the affected OU Director that the oral SWO has been lifted; or
 - (b) Issue a written SWO to the OU Director, with a copy to the responsible line manager, that describes:
 - i. The activity (or activities) covered by the SWO;
 - ii. Interim actions by the OU necessary to protect worker safety and health; and
 - iii. Expectations to be met before consideration will be given to lifting the SWO.
- (4) The CSO will notify the responsible line manager and OU Director in writing when conditions warrant the lifting of a written SWO.

⁶ An oral SWO is not required when, in OSHE's judgment, immediate actions have been taken to eliminate the imminent danger and adequate controls are in place to ensure that the condition is not likely to recur.

d. Communication

- (1) When an employee requests an inspection by OSHE of a perceived imminent danger in an activity other than their own, the employee should notify his or her line management, and when the activity is in another OU, his or her line management should notify the line management of that other OU.
- (2) The responsible line manager, responsible OU Director, and the CSO shall be notified by OSHE as soon as possible of the issuance of an oral SWO.
- (3) The responsible line manager and OU Director shall be notified by OSHE as soon as possible of the lifting of an oral SWO and by the CSO of the issuance and lifting of a written SWO.

7. DEFINITIONS

For definitions common to all NIST OSH suborders, see NIST O 710. Definitions specific to this suborder are as follows:

- a. Imminent Danger (Condition or Practice) – Any serious condition or practice in any workplace which is such that a danger exists which could reasonably be expected to cause death or serious physical harm immediately or before the imminence of such danger can be eliminated through normal procedures.
- b. Serious (Condition or Practice) – A condition or practice in any workplace such that there is a substantial probability that death or serious physical harm could result.
- c. Stop Work Order – Formal notification to cease work activities that present an imminent danger.

8. ACRONYMS

For acronyms common to all NIST OSH suborders, see NIST O 710. Acronyms specific or pertinent to this suborder are:

- a. CFR – Code of Federal Regulations
- b. CSO – Chief Safety Officer
- c. OSH – Occupational Safety and Health

- d. OSHE – Office of Safety, Health, and Environment
- e. OU – Organizational Unit
- f. SWO – Stop-Work Order
- g. UWC – Unsafe or Unhealthful Working Condition.

9. ROLES AND RESPONSIBILITIES

For roles and responsibilities applicable to all NIST OSH programs, see NIST O 710. Roles and responsibilities specific to this suborder are as follows:

a. All Employees:

- (1) Stop their assigned work activities (including work performed by co-workers on the same activity) in accordance with the requirements in Section 6a(2) if they believe that those activities present an imminent danger and they are unable to abate the danger immediately;
- (2) Inform workers performing activities separate from their own (e.g., different project, different OU) of suspected imminent-dangers in a manner that does not increase the danger and recommend that they stop work in accordance with the requirements in Section 6a(2);
- (3) If the workers performing activities separate from their own disagree with their imminent-danger concerns and those concerns persist, immediately report those concerns to the CSO to request an inspection by OSHE; and
- (4) Comply with instructions from co-workers, line managers, or OSHE staff members, including the CSO, to stop work.

b. OU Line Management (in addition to the responsibilities of “All Employees”):

- (1) Ensure that imminent dangers in the workplace are identified and abated; and
- (2) Comply with the applicable requirements in Section 6 and of any oral or written SWOs issued by OSHE or the CSO, respectively.

b. OSHE Staff Members:

- (1) Issue oral SWOs in accordance with the requirements in Section 6c(2) when they identify working conditions that present imminent dangers to one or more persons at any NIST workplace; and
- (2) Notify responsible line managers and OU Directors and the CSO as soon as possible of the issuance of oral SWOs.

c. CSO:

- (1) Evaluate the need for the continuance of oral stop work orders and either lift oral SWOs or issue written SWOs as conditions warrant;
- (2) Lift written SWOs when the imminent dangers have been eliminated and are not likely to recur;
- (3) Ensure that responsible line managers and OU Directors are notified by OSHE as soon as possible of the lifting of oral SWOs and of the issuance and lifting of written SWOs;
- (4) Ensure that information on employees' right and authority to stop work is included in the NIST General Safety Training required by the Safety Education and Training suborder; and
- (5) Ensure that training on the Stop Work suborder is included in the training for line managers, safety and health specialists, and OU/division safety personnel required by the Safety Education and Training suborder.

10. AUTHORITIES

For authorities applicable to all NIST OSH suborders, see NIST O 710. In addition:

a. Employees:

- (1) Stop their assigned work activities if they believe those activities present an imminent danger;
- (2) If imminent-danger concerns persist in their own activities or in the activities of other workers, immediately report those concerns to the CSO to request inspections by OSHE.

b. OSHE Staff Members:

- (3) Issue oral Stop Work Orders when they identify working conditions that present imminent dangers to one or more persons at a NIST workplace.

c. CSO:

- (1) Issue written Stop Work Orders when OSHE staff members identify working conditions that present imminent dangers to one or more persons at a NIST workplace and those conditions have not been eliminated or are likely to recur.

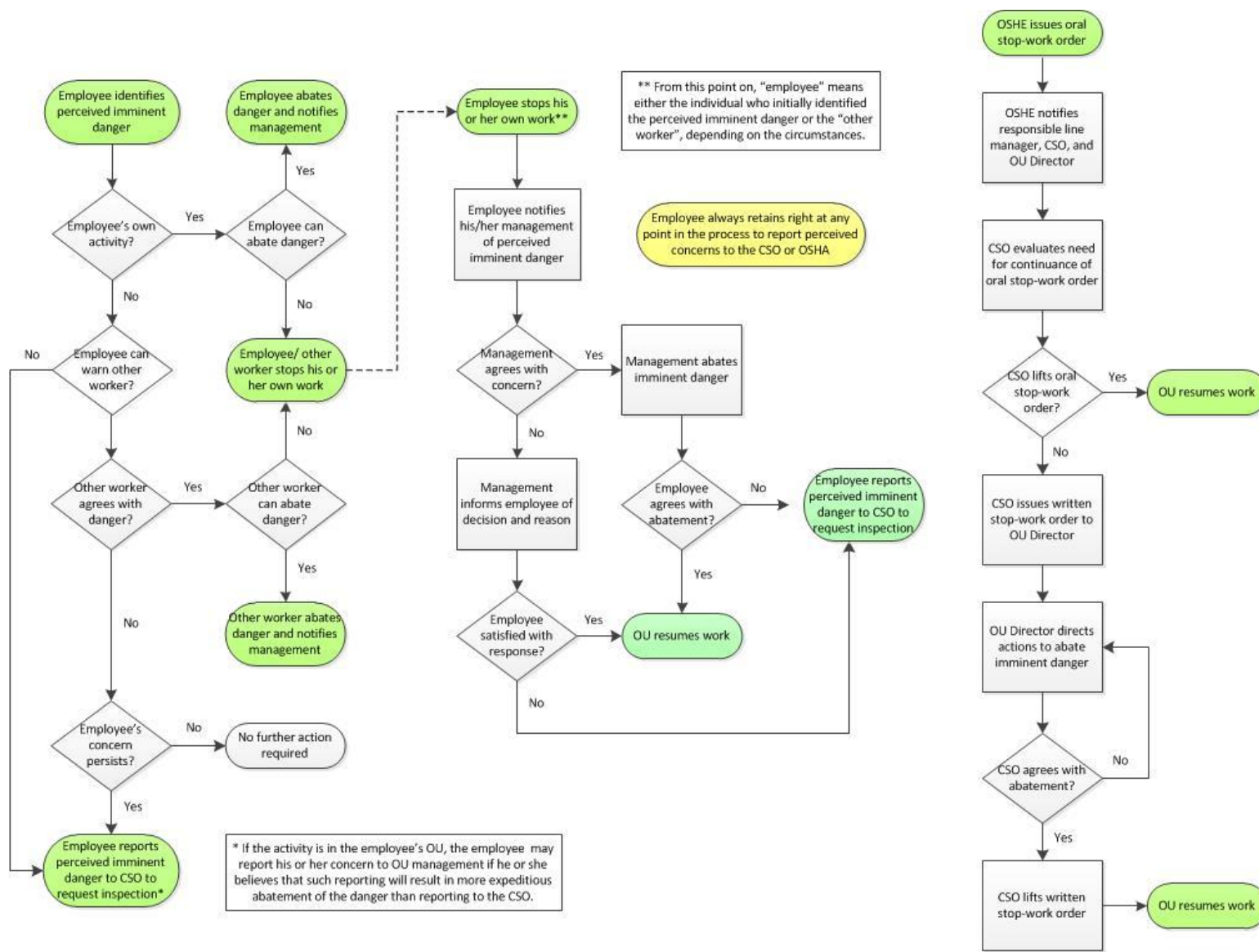
11. DIRECTIVE OWNER

CSO

12. APPENDICES

A. Flow Charts for Employee Stopping Work and OSHE Issuing Stop-Work Orders

Appendix A. Flow Charts for Employees Stopping Work and OSHE Issuing Stop-Work Orders



Safety and Health Requirements for Minors

NIST S 7101.04

Document Approval Date: 05/23/2013

Effective Date: 05/23/2013

1. PURPOSE

To define the safety and health requirements specific to NIST employees and Guest Researchers under age 18, *i.e.*, minors.

2. BACKGROUND

Under certain conditions, qualified minors work at NIST as employees or Guest Researchers. As Guest Researchers, minors participate in the Student Volunteer Program (SVP), including the Summer High School Intern Program (SHIP). If they are college students, minors can also participate in the Summer Undergraduate Research Fellowships Program (SURF) and the Professional Research Experience Program (PREP; Boulder only).

3. APPLICABILITY

- a. This suborder applies to all NIST employees and Guest Researchers under age 18 who could be exposed to hazards while present or conducting work in NIST work areas *other than* offices and office-like spaces (see definition of “Office-Like Space”).
- b. This suborder does not consider regulatory requirements related to hours of work or non-safety-and-health-related conditions of employment.

4. REFERENCES

- a. 29 Code of Federal Regulations (CFR) 570, Child Labor Regulations, Orders, and Statements of Interpretation;

- b. Code of Maryland, Labor and Employment Article, Title 3, Subtitle 2, Employment of Minors;
- c. Colorado Revised Statutes 8-12-110, Hazardous Occupations for Minors;
- d. South Carolina Child Labor Statute, §41-13-20;
- e. 10 CFR 20.1201, Occupational Dose Limits for Adults;
- f. 10 CFR 20.1207, Occupational Dose Limits for Minors; and
- g. 10 CFR 20.1301, Dose Limits for Individual Members of the Public.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews.

6. REQUIREMENTS

- a. General

To work at NIST as an employee, a minor must be at least 16 years of age. To work at NIST as a Guest Researcher, a minor must be at least 14 years of age.

- b. Presence in Work Areas

Minors working at NIST as employees or Guest Researchers are *prohibited* from:

- (1) Being exposed in any work area to recognized hazards that pose a higher than nominal risk to their safety or health (see definition of “Nominal Risk”)¹.
- (2) Being exposed in any work area to ionizing-radiation hazards that could result in their receiving an ionizing radiation dose exceeding the dose limits for members of the public *unless* they have been authorized in accordance with the requirements of the NIST ionizing radiation safety program to engage in work involving ionizing radiation, in which case the occupational dose limits for minors apply (see definition of “Occupational Dose Limits for Minors”).

¹ Note that this does *not* mean that minors cannot be present or work in work areas in which activities are performed that involve hazards that pose a *higher* than nominal risk to safety or health. Minors *may* be present or work in such areas *provided* that (a) the activities in question are not being performed while the minor is present, (b) additional controls are implemented while the minor is present to reduce the risk to the minor’s safety or health to a level that is no higher than nominal, or (c) the minor is asked to leave the work area when those activities are being performed.

c. Work

(1) Minors aged 14 or 15 working at NIST as Guest Researchers are expressly *prohibited* by regulation from engaging in the following:²

- (a) Work involving operating, tending, setting up, adjusting, cleaning, oiling, or repairing hoisting apparatus;
- (b) Work performed in or about boiler or engine rooms or in connection with the maintenance or repair of machines or equipment;
- (c) Work involving operating, tending, setting up, adjusting, cleaning, oiling, or repairing any power-driven machinery, including lawnmowers, golf carts, trimmers, cutters, weed-eaters, and edgers;
- (d) Work involving working from window sills or the use of ladders, scaffolds, or their substitutes;
- (e) Work involving the loading and unloading of goods or property onto or from motor vehicles;
- (f) Occupations in connection with warehousing and storage;
- (g) Occupations in connection with construction, including demolition and repair; and
- (h) Work prohibited for minors aged 16 or 17 (see below).

(2) Minors aged 16 or 17 working at NIST as employees or Guest Researchers are expressly *prohibited* by regulation from engaging in the following:^{2,3}

- (a) Occupations involving the manufacturing, storing, or use of explosives, including articles containing explosive components;
- (b) Occupations involving the manufacturing, storing, or use of radium-containing self-luminous compounds;
- (c) Occupations of motor-vehicle driver and outside helper;

² These prohibitions are headings in 29 CFR 570; for details regarding their meaning, see [29 CFR 570](#).

³ Exemptions to some of these prohibitions are possible under certain circumstances, e.g., if the work is conducted in connection with an established apprenticeship program. For further information, contact OSHE.

- (d) Work involving the operation of power-driven woodworking machines;
- (e) Occupations involved in the operation of power-driven hoisting apparatus;
- (f) Work involving the operation of power-driven metal forming, punching, and shearing machines;
- (g) Work involving the operation of circular saws, band saws, guillotine shears, chain saws, reciprocating saws, wood chippers, and abrasive cutting discs;
- (h) Work involving the erection or repair of electrical wires;
- (i) Occupations involved in wrecking or demolition;
- (j) Work involving roofing operations and being on or about a roof; and
- (k) Work involving excavation operations.

(3) Minors aged 16 or 17 working at NIST as employees and minors aged 14 to 17 working at NIST as Guest Researchers are *permitted* to engage in work not prohibited above provided that:

- (a) Recognized hazards associated with the work and other activities in the work area pose no higher than a nominal risk to their safety and health;
- (b) The work is conducted in full compliance with all applicable NIST and OU safety and health requirements; and
- (c) The work, if it involves ionizing radiation, is conducted in a manner in which occupational radiation dose is kept As Low As is Reasonably Achievable (ALARA) and does not exceed the annual occupational dose limits for minors.

d. Forms

Forms applicable to minors working at NIST as employees or Guest Researchers must be completed by the minors, their parents or guardians, and the NIST OUs in accordance with requirements maintained by the Office of Workforce Management (employees) and the International and Academic Affairs Office (Guest Researchers).

7. DEFINITIONS

- a. Dose Limits for Members of the Public – A total effective dose equivalent from licensed operation of 100 mrem (1 mSv) in a year, or a dose in any unrestricted area from external sources of 2 mrem (0.02 mSv) in any one hour (for details, see 10 CFR 20.1301).
- b. Employee – An individual employed by NIST who has been issued a NIST employee badge.
- c. Guest Researcher – A type of NIST associate.
- d. Host – A NIST employee who is responsible for overseeing the activities of a minor working at NIST as a NIST Guest Researcher.
- e. Minor – Any individual under age 18.
- f. NIST Associate – An individual working at but not employed by NIST. Types of NIST associates include, but are not limited to, foreign and domestic guest researchers and NIST facility users (see <https://inet.nist.gov/tpo/services/upload/NAIS-Types-06022014.pdf>).
- g. Nominal Risk – (a) A risk that is assessed as “Low” or “Minimal” in a hazard review based on the risk-assessment matrix in Appendix A⁴ (or equivalent), or (b) a risk that is assessed as “Medium” and with additional documentation to support accepting the risk for minors.⁵ In both cases, the assessed risk is the risk with all controls⁶ implemented.
- h. Occupational Dose Limits for Adults – (a) The more limiting of a total effective dose equivalent of 5 rem (0.05 Sv) in a year and the sum of the deep-dose equivalent and the committed dose equivalent to any individual organ or tissue other than the lens of the eye of 50 rem (0.5 Sv) in a year; (b) a lens dose equivalent to the eye of 15 rem (0.15 Sv) in a year; and (c) a shallow-dose equivalent of 50 rem (0.5 Sv) to the skin of the whole body or to the skin of any extremity in a year (for details, see 10 CFR 20.1201).
- i. Occupational Dose Limits for Minors – 10% of the annual occupational dose limits for adult workers (see 10 CFR 20.1207 and the definition of “Occupational Dose Limits for Adults”).

⁴ Adapted from ANSI/AIHA Z10-2005, American National Standard – Occupational Health and Safety Management Systems.

⁵ Such documentation could address considerations such as the qualifications of the minor and the implementation of additional controls to reduce the risk to levels that are as low as reasonably achievable, recognizing that the “Medium” level of risk spans a wide range of hazards and risks and that distinctions between “Medium” and “Low” levels of risk are subjective. Such documentation could be part of the hazard review or an addendum to a hazard review.

⁶ Classes of “controls” include engineering controls, administrative controls, and personal protective equipment. Types of administrative control include, but are not limited to, access controls; procedures; training, including on-the-job training; and supervision at a level warranted by the circumstances.

- j. Office-Like Space – A space, such as a conference room, mail room, or computer room that has the same types of hazards as a typical office or office environment.
- k. Organizational Unit (OU) – Term used herein to denote any of the following: the Office of the Director; the immediate offices of the three Associate Directors; the two NIST Centers; the four NIST Laboratories; the three Extramural Programs; and the five Chief Offices.
- l. Work Area – Any space or part of a space in which NIST work is conducted.

8. ACRONYMS

- a. ALARA – As Low As is Reasonably Achievable
- b. CFR – Code of Federal Regulations
- c. OSHE – Office of Safety, Health, and Environment
- d. OU – Organizational Unit
- e. PREP – Professional Research Experience Program (Boulder)
- f. SHIP – Summer High School Intern Program
- g. SURF – Summer Undergraduate Research Fellowships Program
- h. SVP – Student Volunteer Program

9. RESPONSIBILITIES

- a. NIST Supervisors or Hosts:

- (1) Ensure that employees knowledgeable of the hazards to which minors could be exposed while present or working in a work area have performed a hazard review in accordance with the NIST Hazard Analysis and Control Program and applicable OU procedures and have identified the controls necessary to mitigate those risks to the nominal level⁷;
- (2) Ensure that minors are not permitted to engage in work expressly prohibited above;

⁷ Such a hazard review may, if permitted by OU procedures, stand alone, be an addendum to another hazard review, or be part of a hazard review of work of larger scope.

(3) Ensure that work by minors is conducted in full compliance with all applicable NIST and OU safety and health requirements, including requirements resulting from hazard reviews, i.e., for the implementation of controls; and

(4) Ensure that work by minors involving ionizing radiation is conducted in a manner in which occupational ionizing-radiation dose is kept As Low As is Reasonably Achievable (ALARA) and does not exceed the annual occupational dose limits for minors.

b. OU Directors:

(1) When the nominal risk is assessed as “Medium” (see definition of “Nominal Risk”), determining whether the additional documentation provided is sufficient, based on the circumstances, to warrant accepting the risk to the minor, and if it is, signing the documentation indicating their approval.

10. AUTHORITIES

a. OU Directors:

(1) May delegate the authority to accept nominal risks assessed as “Medium” to OU Deputy Directors or Division Chiefs, or, in the case of OUs that do not have Division Chiefs, Division-Chief equivalents⁸.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

a. Appendix A. Risk Assessment Matrix

⁸ The NIST Center for Neutron Research and the Center for Nanoscale Science and Technology do not have Division Chiefs.

Appendix A. Risk Assessment Matrix

		POTENTIAL SEVERITY OF HAZARD			
		Catastrophic Death or permanent disability System or facility loss Lasting environmental or public-health impact	Severe Serious injury; temporary disability Subsystem loss or significant facility/property damage Temporary environmental or public-health impact	Moderate Medical treatment beyond first aid; lost-work-day(s) More than slight facility/property damage External reporting/requirements; more than routine clean-up	Minor First-aid only Negligible or slight facility/property damage No external reporting requirements; routine clean-up
LIKELIHOOD OF OCCURRENCE	Frequent Likely to occur repeatedly	CRITICAL	CRITICAL	SERIOUS	Medium
	Probable Likely to occur multiple but infrequent times	CRITICAL	CRITICAL	SERIOUS	Medium
	Occasional Likely to occur at some time	CRITICAL	SERIOUS	Medium	Low
	Remote Possible, but not likely to occur	SERIOUS	Medium	Medium	Low
	Improbable Very unlikely; can reasonably assume it will not occur	Medium	Low	Low	Minimal

Work and Worker Authorization Based on Hazard Reviews (“Hazard Review”)

NIST S 7101.20

Document Approval Date: 04/18/2014

Effective Date: 04/01/2015

1. PURPOSE

To define the requirements for authorizing both hazardous activities (“work”) and workers based on a systematic level of work planning and control commensurate to the hazards, job complexities, and physical location, *i.e.*, based on hazard reviews.

2. BACKGROUND

- a. This suborder describes NIST’s graded approach to managing the safety of a wide range of hazardous activities, from those that are relatively simple and routine to those that are highly complex one-time projects. The graded approach is based on the severity of the consequences of hazardous events or exposures to hazards and the likelihood of such events or exposures.
- b. This suborder supersedes NIST Administrative Manual Subchapter 12.06, *Hazard Analysis and Control*.

3. APPLICABILITY

- a. The requirements of this suborder apply to all activities conducted by NIST employees and associates as part of their assigned duties except for the following:
 - (1) *Common Everyday Tasks Performed Routinely by Members of the General Public at Work and Home and that Do not Involve Extraordinary Hazards*. This exception recognizes that NIST staff members possess the knowledge, skills, and abilities to perform a wide variety of common everyday tasks safely without written hazard reviews. Examples of such common everyday tasks include working at a computer, reviewing

documents, walking, climbing stairs, picking up objects, and using scissors or short step stools.

(2) *Inherently Low-Risk Activities*. This exception applies to activities that are considered to present low safety risks without NIST personnel having to implement any safety controls to mitigate those risks.^{1,2} The following activities are considered to present low safety risks:

(a) Activities that could result in injuries requiring first aid but only infrequently; and

(b) Activities that could result in injuries requiring medical treatment beyond first aid but are very unlikely to do so.

Examples of inherently low-risk activities include calibrating a balance, preparing non-hazardous solutions, and using an optical microscope to examine non-hazardous samples.

- b. The exemptions provided in Section 3a do not relieve NIST staff members or management from their responsibility to manage the safety risks associated with common everyday tasks and inherently low-risk activities. NIST focuses on these using a variety of mechanisms, including general safety training, safety-related communications, and incident awareness and reduction efforts. In addition, the exemptions do not relieve NIST of its responsibility to evaluate the compatibility of such activities with more hazardous activities in the same spaces.

4. REFERENCES

- a. 29 Code of Federal Regulations 1910.132, Personnel Protective Equipment.

5. APPLICABLE OCCUPATIONAL SAFETY AND HEALTH (OSH) SUBORDERS

- a. NIST S 7101.04: Safety and Health Requirements for Minors;
- b. NIST S 7101.21: Personal Protective Equipment;

¹ This presumes that if such an activity involves the use of equipment with built-in safety features, these features do not require written safe work practices, are not easily defeated, and will not be intentionally defeated or separated from the equipment.

² The requirements of this suborder apply to any activity for which PPE is *required* to mitigate the activity's safety risks. They do not apply to the following uses of PPE: PPE required solely for entry into the space in which the inherently low-risk activity is conducted, not for protection from the hazards associated with the activity; PPE used *voluntarily* as an additional layer of protection; and PPE worn solely to protect equipment or materials.

- c. NIST S 7101.58: Respiratory Protection;
- d. NIST S 7101.55: Hearing Protection;
- e. NIST S 7101.22: Hazard Signage;
- f. Other OSH suborders that contain sections focused on the identification, assessment, and mitigation (*i.e.*, control) of hazards in specific OSH areas, *e.g.*, chemical hazard communication, chemical management, cryogen safety, dispersible engineered nanomaterials, hearing protection, and magnetic-field safety, to name several; and
- g. NIST S 7101.23: Safety Education and Training.

6. REQUIREMENTS

Requirements are provided for the risk-assessment methodology to be used in conducting hazard reviews; the content, conduct, and approval of hazard reviews; the authorization of work and workers; the re-review and re-approval of hazard reviews and the re-authorization of work; retraining and reauthorization of workers; records; activities involving workers from multiple OUs; and Organizational Unit (OU) implementing procedures. Appendix B illustrates the processes for authorizing work and workers and the role of hazard reviews.

a. Risk-Assessment Methodology

Procedures for implementing this suborder shall use the risk-assessment matrix in Appendix C as the basis for conducting risk assessments (see Section 6c). In particular, once a hazard has been identified, the risk of a hazardous event or exposure associated with that hazard shall be characterized, as indicated in Appendix C and below, by an RHI based on the severity of the consequences of a hazardous event or exposure to a hazard and the likelihood of such an event or exposure.

(1) Severity of the consequences of a hazardous event or exposure to a hazard (“Severity”)

- (a) The severity categories in Appendix C provide qualitative measures of the consequences of the worst credible hazardous event (see definition of “Worst Credible Hazardous Event”) or exposure associated with an identified hazard due to design inadequacies; procedural deficiencies; human error; environmental conditions; or system, subsystem, or component failure or malfunction. The severity categories that shall be used are:

- i. CATASTROPHIC: Death or permanent disability; system or facility loss; major property damage, lasting environmental or public-health impact.
- ii. SEVERE: Serious injury; temporary total disability (more than 3 months); subsystem loss or significant facility/property damage, temporary environmental or public-health impact.
- iii. MODERATE: Medical treatment beyond first aid; lost work days; more than slight facility/property damage; external reporting requirements; more than routine clean-up.
- iv. MINOR: First aid or minor medical treatment; negligible or slight facility/property damage; no external (outside NIST) reporting requirements, routine cleanup.

(2) Likelihood of a hazardous event or exposure (“Likelihood”)

- (a) The likelihood categories in Appendix C broadly estimate the probability that a hazardous event or exposure involving an identified hazard will occur in carrying out an activity. The likelihood categories that shall be used are:

- i. FREQUENT: Likely to occur frequently or repeatedly.
- ii. PROBABLE: Likely to occur multiple but infrequent times.
- iii. OCCASIONAL: Likely to occur at some time.
- iv. REMOTE: Possible, but not likely to occur.
- v. IMPROBABLE: Very unlikely: can reasonably be assumed not to occur.

To the extent practical, likelihood should be assigned based on research, analysis, experience, or evaluation of historical safety data from work with similar hazards.

(3) RHIs

- (a) RHIs shall be associated with identified hazards by assigning both severity and likelihood categories as indicated above and by identifying the corresponding RHIs at the intersection of the severity column and likelihood row in the risk-assessment matrix in Appendix C. The RHI levels that shall be used are:

- i. Critical (RHI = 4)
- ii. Serious (RHI = 3)
- iii. Medium (RHI = 2)
- iv. Low (RHI = 1)
- v. Minimal (RHI = 0)

The RHI for an identified hazard provides a measure of the risk associated with that hazard *assuming* that some set of controls has been implemented, where that set of controls could range from inherent/built-in controls only to inherent/built-in controls plus additional controls. In this sense, *RHIs are based on mitigated hazards*.³

b. Hazard-Review Process

Hazard reviews shall consist of the following primary elements, each of which must be documented: (1) activity description, (2) activity hazard identification, (3) physical-location review, (4) compatibility assessment, (5) initial hazard assessment, (6) hazard mitigation, (7) incident-response plan, and (8) risk assessment. Appendix D provides a flowchart illustrating the relationship of these elements.

(1) Activity Description

Hazard reviews shall:

- (a) Fully and accurately describe the activity being reviewed, including its intended outcome or expected result, in a way that is detailed enough for someone outside of the division or group to understand it;⁴
- (b) Define the activity boundaries by identifying what is included in the activity as well as what is specifically excluded from the activity, *e.g.*, commissioning, normal operations, and maintenance of an instrument could be considered separate activities with their own hazard reviews, depending on how different the hazards and associated controls are in the three phases;

³ RHIs are sometimes conceptualized as being based on (a) severity *taking into account inherent/built-in controls only* and (b) likelihood *after the implementation of additional controls*. This is valid to the extent that additional controls reduce, or are considered to reduce, *only* likelihood, *not* severity.

⁴ An activity description similar to a scientific abstract would represent a best management practice.

(c) Identify distinct subtasks within an activity based on significant differences in the nature of the work and associated hazards (hazards may differ from task to task and must be managed accordingly);

(d) Specify the physical location in which the activity is to be conducted; if the activity is to be conducted in multiple locations, describe the general environment in which the activity will be conducted and describe any specific restrictions, if applicable. When the restrictions vary from location to location, subtasks should be assigned by location.

(2) Activity Hazard Identification

The activity hazard identification shall:

(a) Identify the hazards associated with the activity, or, if the activity comprises distinct subtasks, the hazards associated with each of those subtasks; and

(b) Note, reference, or include as attachments to the hazard review the results of any exposure assessments or calculations conducted to characterize or quantify identified potential hazards associated with the activity.

(3) Physical-Location Review

The physical-location review shall determine if the venue in which the activity is to be conducted is appropriate and adequate. Routine laboratory, shop, or mechanical activities are typically acceptable in spaces intended for such activities. OSHE should be consulted, however, when unique, atypical, or unusual activities may not be consistent with the proposed venue, and the results of the consultation should be noted in the review. For example, OSHE should be consulted when the activity involves unusual quantities or classes of hazardous materials or requires specialized fire and life-safety systems or emergency-response equipment, and the results should be noted in the review.

(4) Compatibility Assessment

The compatibility assessment shall examine the hazard reviews associated with the totality of activities conducted in the proposed physical location, both in the actual space itself and, when applicable, neighboring spaces, to identify any potentially negative or antagonistic interactions, taking into account both planned operations and off-normal conditions that could reasonably be expected to occur.

225 (5) Initial Hazard Assessment

226 The initial hazard assessment shall:

- 227
- 228 (a) Identify for each identified hazard the key stages in the activity, or its subtasks, at
229 which a hazardous event or exposure could occur, focusing on those stages essential
230 to safe conduct of the activity or its subtasks; and
- 231
- 232 (b) Assign severity levels to each of the identified hazards, taking into account
233 inherent/built-in controls only, *i.e.*, prior to identifying any other controls (see
234 definition of “Inherent/Built-In Controls”);
- 235
- 236 (c) Take into account any synergistic, negative, or antagonistic interactions identified in
237 the compatibility assessment.
- 238

239 (6) Hazard Mitigation

- 240
- 241 (a) Hazard mitigation shall employ the following “hierarchy of controls” (*i.e.*, preferred
242 order of implementation of controls) to mitigate each of the identified hazards, with
243 each subsequent control category being less effective and reliable than the previous
244 category:
- 245
- 246 i. Elimination;
- 247
- 248 ii. Substitution;
- 249
- 250 iii. Engineering controls;
- 251
- 252 iv. Administrative controls (including signage, warnings, alarms, and training),
253 and;
- 254 v. Personal protective equipment (PPE).
- 255

256 Hierarchy of controls shall be employed until enough controls have been identified to
257 mitigate the hazards to acceptable levels; in some cases, a combination of controls
258 may be necessary, *e.g.*, engineering controls such as machine guarding and local
259 exhaust ventilation could be used in conjunction with training and PPE to mitigate a
260 hazard. There must be a clear connection between the hazards, the controls, and the
261 mitigation of the hazards.

262

- (b) Hazard mitigation shall stipulate the engineering controls required for an activity, *e.g.*, chemical fume hood, gas cabinet, enclosures, interlocks, blast wall, safety interlock.
- (c) Hazard mitigation shall specify the alarms and other warnings required for an activity, *e.g.*, toxic gas alarms, oxygen sensors, warning lights, hazard signage.
- (d) When engineering controls and alarms and other warnings must be integrated into the building infrastructure, the hazard review shall confirm that the physical location in which the activity is to be conducted contains, or will contain, such equipment.
- (e) Hazard mitigation shall specify safe operating guidelines, as applicable (see definition of “Safe Operating Guidelines”), and incorporate these explicitly in the hazard review, either in their entirety or by reference.
- (f) Hazard mitigation shall specify any restrictions on employees conducting activities alone or out of hours, and if there are such restrictions, the additional safety measures that must be implemented, *e.g.*, buddy system, safe operating guideline.
- (g) Hazard mitigation shall specify any ongoing direct supervision required for employees to engage in the activity when ongoing direct supervision is deemed a necessary administrative control.
- (h) Hazard mitigation *should* specify any restrictions on:
- i. The number of hours employees spends on the activity during a work day;
 - ii. The time of day employees conduct the activity; and
 - iii. The environmental conditions under which employees conduct the activity.
- (i) Hazard mitigation shall specify the PPE required for conduct of the activity or subtasks of the activity.
- i. All PPE, including employee-owned PPE, shall be of safe design and construction for the work to be performed.
 - ii. PPE shall be selected in accordance with the requirements in the PPE and other OSH suborders (*e.g.*, Biosafety, Cryogen Safety, Hearing Protection, Respiratory Protection, *etc.*), as applicable.

303 iii. PPE that properly fits each affected employee shall be selected.

304
305 (j) Hazard mitigation shall, based on the physical-location review, identify any
306 additional controls necessary to conduct the activity safely in the proposed physical
307 location.

308
309 (k) Hazard mitigation shall, based on the compatibility assessment, identify any
310 additional controls necessary to conduct the proposed activity safely in proximity to
311 other activities in the space and, when applicable, neighboring spaces.

312
313 (l) Hazard mitigation shall specify the activity-specific training, to be provided by the
314 OU, required for employees to engage in the activity, or distinct subtasks of the
315 activity, in the proposed physical location, and, when applicable, in proximity to other
316 activities in the space and neighboring spaces.

317
318 i. The Safety Education and Training suborder requires employees to complete the
319 training specified in OSH suborders (*e.g.*, Biosafety, Cryogen Safety, Magnetic
320 Fields, *etc.*) applicable to the work they are to conduct. This training is
321 documented and recorded in accordance with the requirements of the Safety
322 Education and Training suborder and need not be specified in the hazard review.

323
324 ii. When activities involve the use of PPE, the activity-specific training must result
325 in employees being able to demonstrate an understanding of the following
326 requirements, and any special activity-specific abilities needed to use the
327 applicable PPE properly, before they are permitted to perform work with that
328 PPE:

329
330 (i) What PPE is necessary;

331
332 (ii) When PPE is necessary;

333
334 (iii) How to properly don, doff, adjust, and wear the PPE;

335
336 (iv) The limitations of the PPE; and,

337
338 (v) The proper care, maintenance, useful life, and disposal of the PPE.

339
340 This activity-specific training must address only those activity-specific aspects of
341 the PPE not covered in either (1) the training provided by OSHE on the PPE
342 program, or (2) the training completed previously by affected employees for other

activities. This training shall be provided by OU employees, or others, who have demonstrated an understanding of the activity-specific aspects of the applicable PPE and any activity-specific ability to use that PPE properly.

- (m) Voluntary use of controls should be documented in the hazard mitigation section of the Hazard Review when such use is subject to requirements in other OSH suborders.⁵

(7) Incident-Response Plan (Activity Specific)

Planning for incidents, including off-normal conditions⁶, as applicable, is a critical element of the hazard review process. In addition to providing guidance during an emergency, the development of incident-response plans may result in the identification of hazardous conditions that could aggravate or compound an emergency situation. Additionally, the planning process may bring to light deficiencies, such as the lack of resources (equipment, trained personnel, supplies) or adequate controls that can be rectified before an emergency occurs. Hazard reviews shall include activity-specific incident-response plans that:

- (a) Stipulate any activity-specific equipment and supplies required for incident response, *e.g.*, emergency shut-off switch, spill containment, special-purpose vacuum cleaner;
- (b) Include the following when necessary to protect employee safety and health, the physical location, and the environment:
 - i. Procedures for shutting down or placing systems in a safe configuration;
 - ii. Plans for responding to off-normal conditions resulting from the failure of one or more controls in the activity itself and, when necessary, other activities conducted in the same space or neighboring spaces;
 - iii. Plans for responding to events such as utility losses, *e.g.*, power or water, and building evacuations; and
 - iv. The identification of additional controls deemed necessary to reduce risks to acceptable levels;

⁵ For example, the voluntary use of respiratory protection is governed by specific requirements in the Respiratory Protection suborder.

⁶ Examples of off-normal conditions, *i.e.*, conditions outside of expected operating limits, include over or under pressure, over or under temperature, over or under flow rates, and loss of electrical power.

(c) Ensure that decisions regarding employees working alone or out of hours fully take into account the need to respond promptly, if necessary, to incidents that threaten employee safety and health or the environment; and

(d) Specify the activity-specific incident-response training, to be provided by the OU, required for employees to engage in the activity or distinct subtasks of the activity.

(8) Risk Assessment

(a) Hazard Reviews shall include an assessment of the risks by assigning RHIs to each of the identified hazards subsequent to the application of controls.

(b) If the risk assessment subsequent to hazard mitigation results in RHIs that feasibly could be lower, additional steps to mitigate the hazards shall be taken to reduce the RHIs to those lower levels.

(9) Additional Requirements

(a) Hazard reviews shall meet the additional requirements established in other OSH suborders, when applicable;⁷

(b) Hazard reviews shall flag, *e.g.*, using checkboxes, activities requiring the control of hazardous energy (lockout/tagout), confined-space entry, hearing protection, respiratory protection, fall protection, and assessments of exposure to carcinogenic chemicals;

(c) Hazard reviews shall be readily available in hard-copy or electronic form in or near the space in which the associated activities are to be conducted; and

(d) Hazard reviews shall identify hazardous wastes generated in the conduct of the activity and include management of those wastes, as applicable. Arrangements for disposal shall be coordinated with OSHE.

c. Conduct of Hazard Reviews

Hazard reviews shall be conducted by, or in consultation with, individuals with the knowledge, skills, and abilities to identify, assess, and mitigate the hazards associated with

⁷ For example, hazard reviews of activities involving the use of biohazardous materials must include a Biohazardous Materials Registration and Authorization Form approved by the NIST Biosafety Officer; hazard reviews of activities involving the use of radioactive material at NIST Gaithersburg must include (among other things) a specific hazard assessment and hazard mitigation plan whose safety evaluation by the NIST Gaithersburg Radiation Safety Officer has been approved by the NIST Ionizing Radiation Safety Committee.

the activity under review, to conduct the physical-location review and compatibility assessment, and to develop plans for incident response.

(1) Hazard reviews shall be conducted by individuals who collectively⁸ have taken the training provided by OSHE on the Hazard Review program and on all OSH programs pertinent to the activity under review.

(2) Hazard reviews should include subject matter experts from OSHE, the Office of Facilities and Property Management (OFPM), and other OUs when the OU conducting the hazard review requires additional safety or facilities expertise.

(3) Hazard reviews shall include consultation with the relevant groups in OFPM (*e.g.*, Police Services, Fire Protection, Plant, Engineering Maintenance and Support Services) when activity-specific alarms must be tied into building or facility alarm systems.

d. Approval of Hazard Reviews^{9, 10}

Completed hazard reviews shall be approved by line management, with the approval signifying that the RHIs associated with the activity represent an acceptable level of safety risk.¹¹

(1) Hazard reviews shall be approved by line managers who have taken the training provided by OSHE on the Hazard Review program.

(2) Activities with any RHI = 4 shall not be conducted at NIST.

(3) Hazard reviews of activities involving minors (individuals under age 18) that could result in their being exposed to hazards with RHI = 2 shall be approved by OU Directors.^{12, 13}

⁸ At least one member of the team must have taken the required training.

⁹ Sections 6d-i focus on activities that involve workers from a single OU. Section 6j indicates how Sections 6d-i apply to activities that involve workers from multiple OUs.

¹⁰ OUs may approve hazard reviews and authorize work at one time provided that the requirements in this section and Section 6e, respectively, are met.

¹¹ The approved hazard review serves as the Certification of Hazard Assessment required by 29 CFR 1910.132, *Personal Protective Equipment*.

¹² As indicated in Section 10. AUTHORITIES, OU Directors may delegate the authority to approve such hazard reviews to OU Deputy Directors or Division Chiefs.

¹³ Activities with RHIs > 2 and a list of other specific activities are prohibited for minors; see the Safety and Health Requirements for Minors suborder.

(4) With the exceptions noted in items (5) and (6) below, all other hazard reviews shall be approved at the following *or higher* levels of the line management of the OU responsible for the activity (see [NIST O 710](#)):¹⁴

(a) Group Leaders:

i. Activities with all RHIs ≤ 1 .

(b) Division Chiefs:

i. Activities with some RHIs = 2 but no RHIs = 3.

(c) OU Directors:¹⁵

i. Activities with at least one RHI = 3.

(5) Activities for which the highest hazards have RHI = 2 and these are fully controlled to industry standards (see definition of “Fully Controlled to Industry Standards”), as determined by OSHE, may be approved by Group Leaders.

(6) Activities for which the highest hazards have RHI = 3 and these are fully-controlled to industry standards (see definition of “Fully Controlled to Industry Standards”), as determined by OSHE in consultation with experts in the OUs, may be approved by Division Chiefs.

e. Authorization of Work¹⁶

Activities covered by approved hazard reviews shall be authorized to commence by line management, with the authorization signifying that controls other than training¹⁷ have been verified to have been implemented and that the controls will continue to be implemented as a condition for the ongoing conduct of the work.¹⁸

¹⁴ OUs may require lower levels of line management (and others, e.g., chairs of hazard review committees, OU/division safety personnel, and project leaders) to sign off on hazard reviews prior to those hazard reviews being approved at the levels of line management indicated.

¹⁵ OU Directors may wish to establish (standing or *ad hoc*) Hazard Review Committees to conduct (or review) hazard reviews for such activities and recommend their approval or disapproval.

¹⁶ OUs may approve hazard reviews and authorize work at one time provided that the requirements in this section and Section 6e, respectively, are met.

¹⁷ Training is addressed not in the authorization of work, but in the authorization of workers; see Section 6f.

¹⁸ So, for example, if a chemical fume hood is a required control, and the chemical fume hood is out of service or suspected to be functioning improperly, the work must stop until the fume hood is fully operational or an equivalent control is identified and implemented. Similarly, PPE must be in good working condition; defective or damaged PPE shall not be used.

(1) Activities shall be authorized by line managers who have taken the training provided by OSHE on the Hazard Review program.

(2) Activities with any RHI =4 shall not be authorized by NIST.

(3) With the exceptions noted in item (4) below, activities covered by all other hazard reviews shall be authorized at the following *or higher* levels of line management:¹⁹

(a) Group Leaders:

i. Activities with all RHIs ≤ 2 .

(b) Division Chiefs:

i. Activities with at least one RHI = 3.

(4) Activities for which the highest hazards have RHI = 3 and these are fully-controlled to industry standards (see definition of “Fully Controlled to Industry Standards”), as determined by OSHE, may be authorized by Group Leaders.

(5) If an activity of one OU is to be conducted in space assigned to another OU, access to that space must be authorized by the line management of the second OU subject to any conditions established by that OU to protect other employees working in the space from the hazards associated with the activity. These conditions must be included as part of the formal authorization of work (see [NIST O 710](#)).

f. Authorization of Workers

To engage in activities that have been authorized by line management, workers must themselves be authorized by line management. This authorization signifies that the workers have taken the training specified in the OSH suborders applicable to the work they are to conduct and the activity-specific training identified in Sections 6b(6)(i) (Hazard Mitigation) and 6b(7)(c) (Incident-Response Plan). It also signifies that line-management has an appropriate degree of confidence, based on personal knowledge, observation, or reliable input from others, that the workers to be authorized have the knowledge, skills, and abilities to perform the work safely and correctly.

¹⁹ OUs may require lower levels of line management (and others, such as chairs of hazard review committees, OU/division safety personnel, and project leaders) to sign off on authorizations of work prior to work being authorized at the level of line management indicated.

- (1) Workers shall be authorized by line managers who have taken the training provided by OSHE on the Hazard Review program and, in the case of official first-level supervisors, on all OSH programs applicable to the work to be conducted;²⁰ and
- (2) Workers shall be authorized by their official first-level supervisors, *or at that level and higher*.^{21, 22}

g. Re-Review and Re-Approval of Hazard Reviews and Re-Authorization of Work and Workers

- (1) Hazard reviews shall be re-reviewed whenever:
- (a) Changes in existing activities, such as changes in scale, materials, equipment, or equipment operation, would introduce new hazards or increase existing hazards;
 - (b) Changes in engineering controls, administrative controls, or PPE would increase safety risks; or
 - (c) Previously unrecognized safety issues are identified, *e.g.*, through direct observation or discussion, or in connection with an incident or audit that indicates inadequate controls.
- (2) Hazard reviews shall be re-reviewed on a predetermined basis to verify that the hazards have not changed substantially since the hazard review was last approved or reviewed, and that existing controls are adequate. Predetermined review periods:
- (a) Shall be established when hazard reviews are initially reviewed and approved and when they are re-reviewed;
 - (b) Shall not exceed three years;
 - (c) Shall be included in the hazard review documentation;

²⁰ The Safety Education and Training suborder requires official first-level supervisors to complete training on the OSH suborders applicable to the work to be conducted by employees they supervise. This training is documented and recorded in accordance with the requirements of the Safety Education and Training suborder and need not be specified in the hazard review.

²¹ If a worker is to be authorized to carry out only a specified set of subtasks of a larger activity, that worker need only take the training applicable to that specified set of subtasks.

²² If an activity involves workers from one or more groups or divisions within a single OU, the OU may wish to establish additional requirements for authorizing workers across organizational lines. For example, if an activity owned by one group involves workers from a second group and the two Group Leaders are the official first-level supervisors, the OU may wish to have the workers from the second group authorized first by their Group Leader and then by the Group Leader of the group that owns the activity.

(d) Shall be based on risk and the potential for change, with higher-risk, more potentially variable activities being reviewed more frequently; and

(e) May be more frequent based on the likelihood for change within an activity.

(3) When re-reviews indicate that hazards *have not* changed *and* that existing controls are *adequate*, the re-reviewed hazard reviews shall include the date of the re-review, the signature(s) of the individual(s) conducting the re-review, and the signature of the responsible line manager.

(4) When re-reviews indicate that hazards *have* changed *or* that existing controls are *inadequate*:

(a) The re-reviewed hazard reviews shall be re-approved in accordance with the requirements in Section 6d; and

(b) Work and workers shall be re-authorized in accordance with the requirements in Sections 6e and 6f, respectively.

The re-approval of the hazard review and the re-authorization of work shall take place at the levels of line management determined by the hazards that have changed or for which the existing controls are inadequate, or at a higher level of line management.

h. Retraining and Re-Authorization of Workers

(1) Employees who have been authorized to conduct work shall, as a condition of their authorization, complete retraining identified by the OUs whenever there is reason to believe that employees lack the knowledge, understanding, or skill necessary to conduct their work safely. Individual OSH suborders list specific circumstances under which such retraining is required. General circumstances under which retraining is required include, but are not limited to:

(a) An observation or other condition reveals that a worker lacks the necessary knowledge understanding or skill; or

(b) An inspection or audit points to a systemic deficiency warranting retraining.

i. Records

- 579 (1) Copies of all current hazard reviews and work and worker authorizations shall be
580 maintained in hard copy or electronic form.
581
- 582 (2) Copies of hazard reviews and work and worker authorizations for activities that have
583 ceased shall be maintained in hard copy or electronic form for at least one (1) year unless
584 the hazard assessment involved exposure monitoring, in which case the hazard review
585 and work and worker authorizations shall be submitted to OSHE for retention in
586 accordance with the requirements of the Industrial Hygiene program.
- 587 (3) Training shall be documented and recorded in accordance with the requirements, roles,
588 and responsibilities in the Safety Education and Training suborder.
589

590 j. Activities Involving Workers from Multiple OUs
591

- 592 (1) The activity shall be owned by the *de facto* lead OU or, if it is not obvious which OU is
593 the *de facto* lead OU, by the OU determined to be the lead OU by discussion among the
594 involved OUs.
- 595 (2) The hazard review shall be approved by the lead OU in accordance with the
596 requirements in Section 6d, Approval of Hazard Reviews.
597
- 598 (3) Work shall be authorized by the lead OU in accordance with the requirements in Section
599 6e, Authorization of Work.
600
- 601 (4) Workers from the lead OU shall be authorized by the lead OU in accordance with the
602 requirements in Section 6f, Authorization of Workers.
603
- 604 (5) Workers from OUs other than the lead OU shall be authorized by their respective OUs
605 in accordance with the requirements in Section 6f *and* by the lead OU (“final
606 authorization”) in accordance with its own requirements.
607
- 608 (a) In authorizing workers from their OUs, OUs other than the lead OU should
609 determine that the hazard review is adequate, that the safety risk to workers from
610 their OUs is acceptable, and that the work has been authorized by the lead OU.
611
- 612 (6) Hazard reviews shall be re-reviewed and re-approved and work and workers from the
613 lead OU shall be re-authorized by the lead OU in accordance with the requirements in
614 Section 6g, Re-Review and Re-Approval of Hazard Reviews and Re-Authorization of
615 Work and Workers.
616

- (7) Workers from OUs other than the lead OU shall be re-authorized by their respective OUs in accordance with the requirements in Section 6g *and* by the lead OU (“final re-authorization”) in accordance with its own requirements.
- (8) Workers from the lead OU shall be retrained and re-authorized by the lead OU in accordance with the requirements in Section 6h, Retraining and Re-Authorization of Workers.
- (9) Workers from other than the lead OU shall be retrained and re-authorized by their respective OUs in accordance with the requirements in Section 6h *and* by the lead OU in accordance with its own requirements.
- (10) Records related to hazard-review documentation, the authorization of work, and the authorization of workers from the lead OU shall be maintained by the lead OU in accordance with the requirements in Section 6i, Records.
- (11) Records of the authorization of workers from OUs other than the lead OU shall be maintained as follows:
- (a) Records of the authorization of workers from OUs other than the lead OU shall be maintained by the workers’ respective OUs; and
 - (b) Records of the final authorizations of such workers by the lead OU shall be maintained by the lead OU.
- k. OU Hazard Review and Work and Worker Authorization Procedures
- Written procedures, which, if followed, would result in the requirements in Sections 6a-j being met, shall be developed and maintained by each OU.

7. DEFINITIONS

- a. Activity – An experiment, operation, process, or job, often comprising subtasks, conducted to achieve a specific outcome.
- b. Direct Supervision – Relative to an employee, a term meaning that the a second employee, proficient in the activity being conducted by the first employee, shall be either present in the work area while the activity is being conducted or available for consultation within a reasonable amount of time commensurate with the need for consultation, based on the proficiency of the first employee.

- c. Fully Controlled to Industry Standards (Used in Reference to Hazards) – Controlled by virtue of a device, apparatus, or system being designed in accordance with applicable regulatory and consensus standards and predicated upon that device, apparatus, or system being used in a prescribed manner. The mitigation of hazards that are fully controlled to industry standards relies primarily on built-in/engineering controls or inherent design features but may, in some cases, rely upon best practices. In either case, the control should be traceable to a broad industry, consensus-based set of controls.
- d. Hazard – Source, situation, or act with a potential for harm in terms of human injury or ill health, adverse impact on the environment, damage or loss of equipment or property, or a combination of these (from [NIST O 710](#)).²³
- e. Hazard Identification – Process of recognizing that a hazard exists and defining its characteristics (from [NIST O 710](#)).
- f. Hazard Review (Document) – A document describing the results of the hazard-review process.
- g. Hazard Review (Process) – The formal process, aspects of which could be iterative, of describing an activity, identifying the hazards associated with the activity, reviewing the physical-location in which the activity will be carried out, assessing the compatibility of the activity with nearby activities, conducting an initial hazard assessment, identifying controls to mitigate the hazards, developing an incident-response plan, conducting a risk assessment, and developing plans for managing wastes generated during the conduct of the activity.
- h. Hierarchy of Controls – A range of hazard control methods arranged in order of implementation preference from elimination to substitution, engineering controls, administrative controls, and personal protective equipment.
- i. Inherent/Built-In Controls – Features of a system's design that prevent or limit the severity of the consequences of system failure. Inherent/built-in controls cannot be defeated or separated from the system without conscious or willful effort.

²³ This definition parallels that in *Occupational Health and Safety Assessment Series (OHSAS) Standard 18001:2007, Occupational Health and Safety Management Systems – Requirements*. For comparison, *OSHA 3071, Job Hazard Analysis, 2002 (revised)* defines a hazard as “the potential for harm, often associated with a condition or activity that, if left uncontrolled, can result in injury, illness or damage to property or the environment”, and *American National Standard for Occupational Safety and Health Management Systems, ANSI/AIHA Z10-2005*, defines a hazard as “a condition, set of circumstances, or inherent property that can cause injury, illness or death”.

- j. Likelihood of a Hazardous Event or Exposure (“Likelihood”) – An estimate of the probability of a hazardous event or exposure.
- k. Line Management – For the purposes of this suborder, the OU Director, Division Chief, and Group Leader, or equivalent.
- l. Office-Like Space – A space, such as a conference room, copier room, break room, or ordinary computer room that has the same types of hazards as a typical office or office environment.
- m. Off-Normal Conditions – Operational occurrences which may be expected to occur that are generally outside routine or planned operations. Any one or more process variables that will cause some or all of the remaining conditions to become abnormal. For example, loss of cooling water would be an “off-normal” condition which could cause a heat-sink to overheat and combust. Other examples include power failure, error at power-up or power-down, loss of cryogen containment, human error, *etc.*
- n. Relative Hazard Index (RHI) – A measure of the risk of a hazardous event or exposure based on a combination of the severity of the consequences of the hazardous event or exposure to a hazard and its likelihood.
- o. Risk – Combination of the likelihood of an occurrence of a hazardous event or exposure and the severity of injury or ill health that can be caused by the event or exposure (from [NIST O 710](#)).
- p. Risk Assessment – Process of evaluating the risks arising from hazards, taking into account the adequacy of any existing controls, and deciding whether or not the risks are acceptable (from [NIST O 710](#)).
- q. Safe Operating Guideline – A written set of requirements or practices developed or designed to enable a task to be carried out safely. Safe operating guidelines can include, but are not limited to, standard operating procedures, job hazard analyses, and instrument/equipment instruction manuals.
- r. Severity of the Consequences of a Hazardous Event or Exposure to a Hazard (“Severity”) – A qualitative measure of the consequences of the worst credible hazardous event or exposure associated with an identified hazard due to design inadequacies; procedural deficiencies; human error; environmental conditions; or system, subsystem, or component failure or malfunction.

s. Standard Operating Procedure – A written step-by-step procedure or operational protocol used to document how a given task **must** be carried out to ensure safe operation. Standard operating procedures are generally needed when failure to follow a prescribed set of steps results in significant increase in risk.

t. Worst Credible Hazardous Event – Most severe or serious event capable of being believed taking into account all relevant considerations.

8. ACRONYMS

a. HR – Hazard Review

b. OSH – Occupational Safety and Health

c. OSHE – Office of Safety, Health, and Environment

d. OU – Organizational Unit

e. PPE – Personal Protective Equipment

f. RHI – Relative Hazard Index

9. ROLES AND RESPONSIBILITIES

a. NIST Director and Associate Directors:

(1) Concur or non-concur on approvals by OU Directors of hazard reviews of activities elevated to the directorship level.

b. OU Directors:

(1) Ensure that written OU procedures are developed, maintained, and implemented to ensure that the requirements of Sections 6a-j are met within their respective OUs.

c. Line Management:

(1) Take the training provided by OSHE on the Hazard Review program;

(2) Ensure that hazard reviews are conducted for all new activities;

- (3) Involve employees in the conduct of hazard reviews as appropriate;
- (4) Ensure that hazard reviews are conducted by individuals who collectively have taken the training provided by OSHE on the Hazard Review program and on all NIST OSH programs pertinent to the activity under review;
- (5) Approve hazard reviews in accordance with the requirements of Section 6d, with the approval signifying that the RHIs associated with the activity represent an acceptable level of risk;
- (6) Authorize activities in accordance with the requirements of Section 6e, with the authorization signifying that controls other than training have been verified to have been implemented and that required safety equipment shall be maintained in proper working order in accordance with manufacturers' specifications and all applicable standards;
- (7) Authorize workers in accordance with the requirements of Section 6f, with the authorization signifying that (a) the workers have taken the training provided by OSHE on all NIST OSH programs pertinent to the activity to be conducted and the training identified in Sections 6b(6)i (Hazard Mitigation) and 6b(7)c (Incident-Response Plan), and (b) line management has an appropriate degree of confidence, based on personal knowledge, observation, or reliable input from others, that the workers to be authorized have the knowledge, skills, and abilities to perform the work safely and correctly;
- (8) Re-review and re-approve hazard reviews and re-authorize work and workers in accordance with the requirements of Section 6g; and
- (9) Maintain records in accordance with the requirements of Section 6h.

d. Official First-Level Supervisors Authorizing Work (in addition to their responsibilities as part of Line Management):

- (1) Complete the training provided by OSHE on all NIST OSH programs pertinent to the work to be authorized.

e. Employees Conducting Hazard Reviews:

- (1) Take the training provided by OSHE on the Hazard Review program.

f. Employees Authorized to Engage in Work:

(1) Complete the training provided by OSHE on all NIST OSH programs pertinent to the work to be conducted and the training provided by the OU identified in Sections 6b(6)(i) (Hazard Mitigation) and 6b(7)(c) (Incident-Response Plan), as applicable; and

(2) Conduct the work in accordance with their training, and, in particular, ensure that all controls required by the approved hazard review are implemented.

g. Employees Assigned Responsibility for Safety Equipment:

(1) Ensure that required safety equipment is maintained in proper working order in accordance with manufacturers' specifications and all applicable standards.

h. Employees:

(1) Participate in the conduct of hazard reviews as appropriate.

i. Chief Safety Officer:

(1) Maintain this suborder;

(2) Develop and maintain any necessary supporting NIST directives, including procedures, guidance, and notices;

(3) Review the efficacy of written OU procedures for meeting the requirements of this suborder and provide the results of those reviews to the respective OU Directors; and

(4) Support, through the OSHE staff, OU implementation of this suborder.

j. OSH Program Manager for the Hazard Review program:

(1) Make determinations that particular hazards are controlled to industry standards and maintain and make available to the OUs a list of such hazards and their associated RHIs;

(2) Develop and maintain any necessary deployment tools, including forms, instructions, IT applications, training, and user guides;

(3) Serve as the primary point of contact and subject matter expert on:

(a) Federal, State and local regulatory requirements and guidelines; and

(b) Consensus industry standards and best practices.

(4) Ensure effective communication with management and staff on program-related issues.

10. AUTHORITIES

For authorities applicable to all NIST OSH suborders, see [NIST O 710](#). There are no authorities specific to this suborder alone.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

a. Appendix A. Revision History

b. Appendix B. Processes for Authorizing Work and Workers

c. Appendix C. Risk-Assessment Matrix

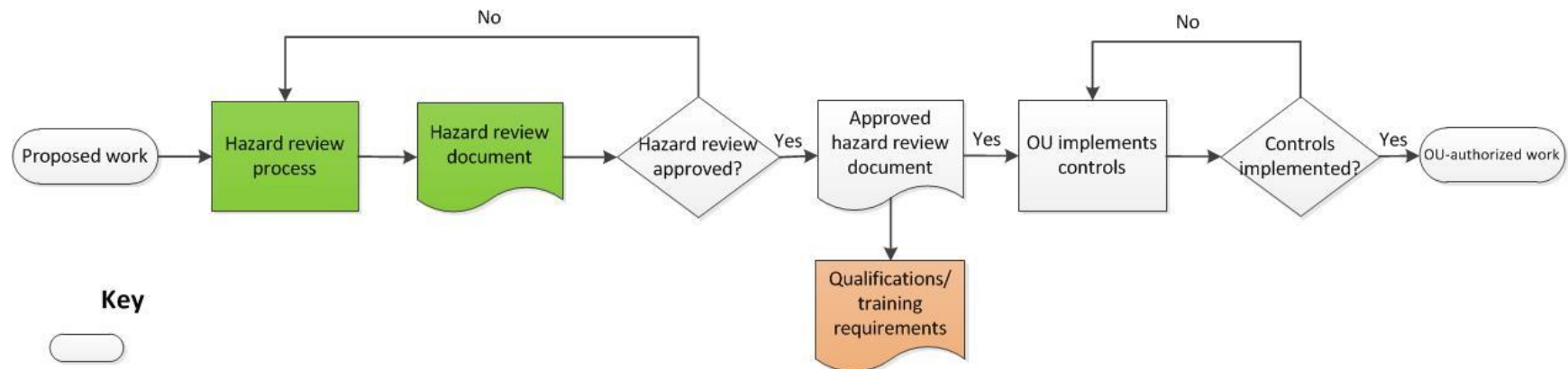
d. Appendix D. Elements of the Hazard Review Process

Appendix A. Revision History

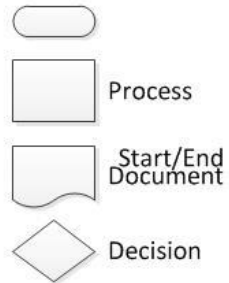
Revision	Date	Responsible Person	Description of Change
1	01/23/15	Richard Kayser	Modifications made to Section 3. Applicability, subsequent to Executive Safety Committee review.

Appendix B. Processes for Authorizing Work and Workers (for details on the hazard-review process, see Appendix D)

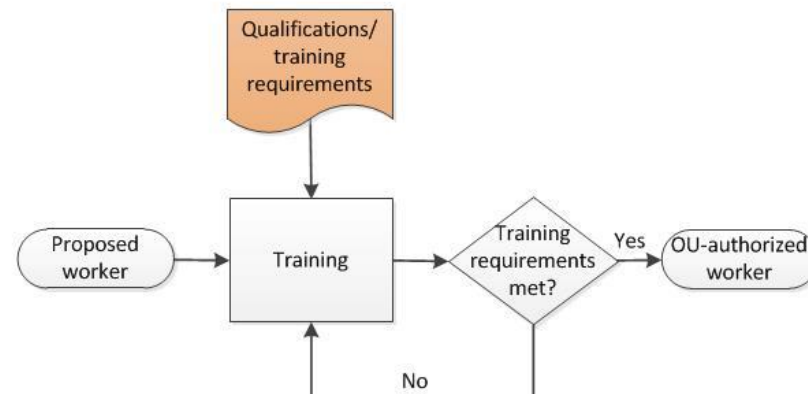
Authorization of Work



Key



Authorization of Workers

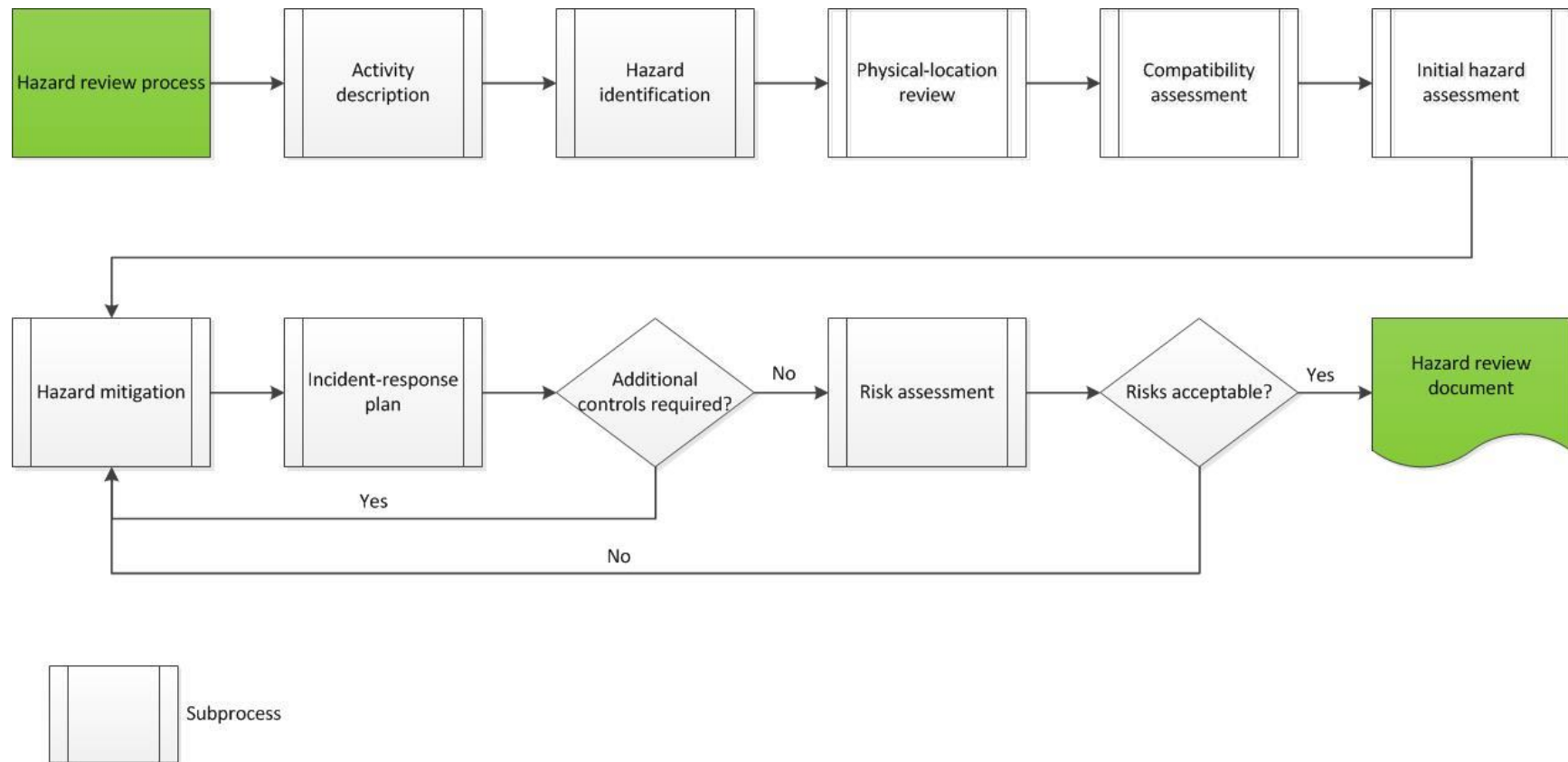


Appendix C. Risk-Assessment Matrix

This matrix is used to determine the risk level, or Relative Hazard Index (RHI), for a given hazard.

		POTENTIAL SEVERITY OF THE CONSEQUENCES OF A HAZARDOUS EVENT OR EXPOSURE TO A HAZARD			
		Catastrophic Death or permanent disability System or facility loss Lasting environmental or public-health impact	Severe Serious injury; temporary disability Subsystem loss or significant facility/property damage Temporary environmental or public-health impact	Moderate Medical treatment beyond first aid; lost-work-day(s) More than slight facility/property damage External reporting requirements; more than routine clean-up	Minor First-aid only Negligible or slight facility/property damage No external reporting requirements; routine clean-up
LIKELIHOOD OF OCCURRENCE	Frequent Likely to occur repeatedly	CRITICAL RHI=4	CRITICAL RHI=4	SERIOUS RHI=3	Medium RHI=2
	Probable Likely to occur multiple but infrequent times	CRITICAL RHI=4	CRITICAL RHI=4	SERIOUS RHI=3	Medium RHI=2
	Occasional Likely to occur at some time	CRITICAL RHI=4	SERIOUS RHI=3	Medium RHI=2	Low RHI=1
	Remote Possible, but not likely to occur	SERIOUS RHI=3	Medium RHI=2	Medium RHI=2	Low RHI=1
	Improbable Very unlikely; can reasonably assume it will not occur	Medium RHI=2	Low RHI=1	Low RHI=1	Minimal RHI=0

Appendix D. Elements of the Hazard Review Process (see Section 6b)



Personal Protective Equipment (PPE)

NIST S 7101.21

Approval Date: 11/13/2015

Effective Date:¹ 11/13/2015

1. PURPOSE

This suborder establishes the safety requirements for personal protective equipment (PPE) necessary to protect NIST employees and associates from exposure to hazardous chemical, mechanical, biological, and other hazards at NIST.

2. BACKGROUND

a. The PPE suborder supports the implementation of the Work and Worker Authorization Based on Hazard Reviews (“Hazard Review”) suborder when it is determined through the hazard-review process that PPE is necessary to protect the safety and health of employees and associates.

b. NIST must meet or exceed the requirements established by the Occupational Safety and Health Administration (OSHA) in [29 CFR 1910.132](#), Personal Protective Equipment – General Requirements.

(1) NIST has integrated the requirements of 29 CFR 1910.132(d), Hazard Assessment and Equipment Selection, and 29 CFR 1910.132(f), Training, into the Hazard Review suborder and fulfills those requirements through the implementation of that suborder.

(2) NIST fulfills the remaining requirements of [29 CFR 1910.132](#) through the implementation of this suborder in conjunction with the Hazard Review suborder.

c. NIST must meet or exceed the requirements established by OSHA in the following standards:

(1) [29 CFR 1910.133](#), Eye and Face Protection;

¹ For revision history, see Appendix A.

- (2) [29 CFR 1910.135](#), Head Protection;
- (3) [29 CFR 1910.136](#), Foot Protection;
- (4) [29 CFR 1910.138](#), Hand Protection;
- (5) [29 CFR 1910.137](#), Electrical Protective Equipment;
- (6) [29 CFR 1926.95](#), Criteria for Personal Protective Equipment;
- (7) [29 CFR 1926.102](#), Eye and Face Protection;
- (8) [29 CFR 1926.100](#), Head Protection; and
- (9) [29 CFR 1926.96](#), Occupational Foot Protection.

NIST fulfills these requirements through the implementation of this suborder in conjunction with the Hazard Review suborder.

- d. NIST must meet or exceed the requirements established by OSHA in [29 CFR 1910.134](#), Respiratory Protection. NIST fulfills those requirements through the implementation of the Respiratory Protection suborder in conjunction with the Hazard Review suborder.
- e. NIST must meet or exceed the requirements established by OSHA in [29 CFR 1910.95](#), Occupational Noise Exposure and [29 CFR 1926.101](#), Hearing Protection. NIST fulfills those requirements through the implementation of the Hearing Protection suborder in conjunction with the Hazard Review suborder.
- f. This suborder supersedes the following NIST Health and Safety Instructions (HSIs):
- (1) HSI 11, Eye Protection Program, December 2004; and
- (2) HSI 12, Foot Protection, September 1999.

3. APPLICABILITY

The provisions of this suborder apply to all NIST employees and associates engaged in activities in which they are required to, or voluntarily, use PPE.

78 **4. REFERENCES**

- 79 a. [29 CFR 1910.132](#), General Requirements;
80
81 b. [29 CFR 1910.133](#), Eye and Face Protection;
82
83 c. [29 CFR 1910.135](#), Head Protection;
84
85 d. [29 CFR 1910.136](#), Foot Protection;
86
87 e. [29 CFR 1910.138](#), Hand Protection;
88
89 f. [29 CFR 1910.137](#), Electrical Protective Equipment;
90
91 g. [29 CFR 1910.134](#), Respiratory Protection;
92
93 h. [29 CFR 1910.95](#), Occupational Noise Exposure
94
95 i. [29 CFR 1926.95](#), Criteria for Personal Protective Equipment;
96
97 j. [29 CFR 1926.102](#), Eye and Face Protection;
98
99 k. [29 CFR 1926.100](#), Head Protection;
100
101 l. [29 CFR 1926.96](#), Occupational Foot Protection;
102
103 m. [29 CFR 1926.101](#), Hearing Protection;
104
105 n. American National Standard, Occupational and Educational Eye and Face Protection, ANSI
106 Z87.1-1989 (or more recent version);
107
108 o. American National Standard, Head Protection, ANSI Z89.1-1986 (or more recent version);
109
110 p. American National Standard, Anti-Vibration Gloves, ANSI S3.40 - 2002 / EN ISO 10819 (or
111 more recent version);
112
113 q. American National Standard, Foot Protection, ANSI Z41.1-1991 (or more recent version);
114
115 r. ASTM International, Standard Specification for Performance Requirements for Foot
116 Protection, ASTM F2413-2005 (or more recent version).
117

118 **5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS**

- 119 a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews; and
120
121 b. Other OSH suborders addressing the need for PPE in specific safety areas, such as biosafety,
122 bloodborne pathogens, cryogens, dispersible engineered nanomaterials, respiratory
123 protection, and hearing protection.
124

125
126 **6. REQUIREMENTS**

127 a. General PPE Requirements
128

- 129 (1) Employee- and associate-provided PPE shall be adequate for the workplace hazards and
130 properly cleaned and maintained.
131
132 (2) All PPE shall be of safe design and construction for the work to be performed.
133
134 (3) PPE shall not create greater risks than those its use is intended to mitigate.
135
136 (4) PPE shall be inspected, cleaned, and maintained in accordance manufacturers'
137 instructions.
138
139 (5) PPE should be distributed for individual use whenever practical.
140
141 (6) PPE shall not be shared among employees and associates until it has been properly
142 cleaned and sanitized as necessary based on the type of PPE.
143
144 (7) Defective or damaged PPE shall not be used.
145
146 (8) PPE that is contaminated, or suspected of being contaminated, with hazardous substances
147 shall not be removed from the work area.
148
149 (9) Contaminated PPE that cannot be decontaminated shall be disposed of in a manner that
150 protects employees, associates, and the environment.
151

152 b. Specific PPE Requirements
153

- 154 (1) Eye and Face Protection

Eye and face protection² meeting the requirements of ANSI Z87.1 must be used when there is the potential to be exposed to eye or face hazards from flying particles, molten metal, liquid chemicals, acids or caustics, chemical gases or vapors, biological hazards, or potentially hazardous light radiation. Specifically:

(a) For potential flying-object hazards, eye protection shall include side-protection.

When detachable side protectors are employed, the combination of glasses and side protectors must be ANSI Z87.1 compliant.³

(b) For potential severe chemical splash hazards, a face shield in combination with primary safety eyewear, i.e., goggles or safety glasses with side shields, shall be worn.

(c) For potential severe exposure to flying fragments or objects, hot sparks from furnace operations, potential splash from molten metal, or extreme temperatures, a face shield in combination with primary safety eyewear shall be worn.

(d) For potential exposure to light radiation other than laser light,⁴ filter lenses that have a shade number appropriate for the work being performed shall be worn; tinted and shaded lenses are not filter lenses unless they are marked or identified as such.

(2) Prescription lenses, when used as, or in conjunction with, safety eyewear, must:

(a) Incorporate the prescription into safety eyewear meeting the requirements of ANSI Z87.1; or

(b) Be worn under ANSI Z87.1 safety eyewear without disturbing the proper position of the prescription lenses or the safety eyewear.

(3) Head Protection

(a) Head protection meeting the requirements of ANSI Z89.1 must be worn when working in areas where there is a potential for a head injury caused by falling objects or impact.

² ANSI Z87.1 does not apply to hazards related to X-rays, gamma rays, high-energy particulate radiation, microwaves, radio-frequency radiation, or work with lasers and masers. Information on PPE required for work involving these hazards is available in other OSH programs.

³ Uncertified prescription or non-prescription glasses are not acceptable when eye protection is required.

⁴ For protection from laser light, refer to [Health and Safety Instruction 13, Laser Safety](#).

- 190 (b) Head protection designed to reduce electrical shock hazards must be worn when
191 working near exposed electrical conductors that could come in contact with the head.
192
- 193 (c) Persons working above other work levels must wear protective helmets with
194 chinstraps designed to prevent the helmets from being bumped off the worker's head,
195 but the chinstraps must not be so strong as to present a strangulation hazard.
196
- 197 (d) Bump caps may be used when head protection is not required but a worker may be
198 exposed to minor head bumps or laceration hazards. Bump caps are not approved for
199 use where impact protection is required.
200

201 (4) Foot Protection 202

- 203 (a) Foot protection meeting the requirements of ASTM F-2413-2005 must be worn when
204 working in areas where there is a danger of foot injury due to hazards such as falling
205 or rolling objects, objects piercing the sole, or electrical hazards.
206
- 207 (b) Shoes resistant to permeation shall be worn at all times in spaces where there is a
208 reasonable likelihood that feet could be exposed to chemicals or materials hazardous
209 to the feet, e.g., toxic chemicals, strong acids or bases, or biohazardous materials.
210
- 211 (c) Perforated shoes, open-toed shoes, sandals, and cloth sneakers shall not be worn in
212 work areas when a more substantial barrier is required to protect workers from
213 surrounding hazards.
214
- 215 (d) Chemical resistant overshoes or boots may be used to avoid possible exposures to
216 corrosive chemicals or large quantities of solvents or solutions that might penetrate
217 normal footwear, e.g., during spill cleanup.
218
- 219 (e) Workers who, for medical reasons, cannot wear required safety shoes, must, upon
220 request, furnish a letter to their supervisor from their physician stating the medical
221 reasons and the anticipated duration of the medical condition. Such workers may
222 wear steel-toe overshoes or toe guards over regular work shoes.
223
224
225
226
227
228
229

230 (5) Hand Protection

231 Hand protection must be worn⁵ when working in areas where there is a danger of hand
232 injury from chemical, biological, cutting, piercing, electrical, or other hazards. Activities
233 requiring the use of hand protection include, but are not limited to:

234
235 (a) Work with harmful substances that can be absorbed through the skin or that can cause
236 skin irritation, chemical burns, or similar conditions, as determined by the activity
237 hazard review. Examples include strong acids or bases and organic solvents. The
238 Safety Data Sheet (SDS) or other product information must be consulted to determine
239 the type of hand protection needed.

240
241 (b) Work with tools, equipment, or materials that can cause cuts, lacerations, punctures,
242 fractures, amputations, or abrasions.

243
244 (c) Work with materials or agents, such as cryogenics, when there is a danger of injurious
245 exposure to harmful temperature extremes.

246
247 (6) Protective Clothing and Body Protection

248
249 (a) Body protection must be provided for workers who are exposed to bodily injury while
250 performing their jobs when engineering and administrative controls, including work
251 practices, have failed to reduce the risks associated with the hazards to an acceptable
252 level. Hazards requiring the use of protective clothing or body protection include, but
253 are not limited to:

254
255 i. Exposure to intense heat or cold (excluding cold weather clothing, which is not
256 covered by this suborder);

257
258 ii. Splashes of very cold or very hot metals or liquids;

259
260 iii. Impacts from tools, machinery, or materials;

261
262 iv. Contact with equipment that could result in cuts or abrasion;

263
264 v. Exposure to hazardous chemicals (consult SDSs for recommended clothing for
265 particular hazardous chemicals);

266

⁵ Use of gloves may not be required and may be prohibited when working with machines such as lathes and drill presses where the glove could become entangled in the equipment and present a greater hazard than the equipment itself.

- 267 vi. Contact with potentially infectious materials, such as blood; and
268
269 vii. Exposure to electrical arc hazards.
270
- 271 c. Training
272
- 273 (1) Employees and associates who are to engage in activities in which they use PPE shall
274 complete:
275
- 276 (a) The training provided by OSHE on the PPE program, which shall include:
277
- 278 i. An overview of the general requirements of the PPE program and associated roles
279 and responsibilities;
280
- 281 ii. Training on the types of PPE applicable to their assigned duties, e.g., hand
282 protection; and
283
- 284 iii. Other relevant safety information; and
285
- 286 (b) The activity-specific training, provided by the OUs, required by hazard reviews.
287
- 288 (2) Official First-Level Supervisors of employees and associates engaged in activities in
289 which they use PPE shall complete the training provided by OSHE on the PPE program,
290 which shall include:
291
- 292 (a) An overview of the general requirements of the PPE program and associated roles
293 and responsibilities;
294
- 295 (b) Training on the types of PPE applicable to the assigned duties of the employees and
296 associates they supervise; and
297
- 298 (c) Other relevant safety information.
299
- 300 (3) Retraining
301
- 302 (a) Employees and associates who have already been trained shall complete retraining
303 identified by the OUs whenever there is reason to believe that employees or
304 associates do not have the understanding and skill necessary to use, care for,
305 maintain, and dispose of PPE properly. Circumstances where retraining is required
306 include, but are not limited to:

- 307 i. Changes in the workplace, or in the type of PPE to be used, render previous
308 training obsolete; or
309
- 310 ii. Inadequacies in an employee's or associate's knowledge or use of assigned PPE
311 indicate that the employee or associate has not retained the necessary
312 understanding or skill.
313
- 314 (3) Documentation and Records
315
- 316 (a) Training shall be documented and recorded in accordance with the requirements,
317 roles, and responsibilities in the Safety Education and Training suborder.
318
- 319 d. Payment for Personal Protective Equipment
320
- 321 (1) PPE used to comply with the requirements of this and other applicable OSH suborders
322 shall be provided by the OUs at no cost to employees or associates.^{6,7}
323
- 324 (a) OUs are not obligated to, but may, provide the following items to NIST employees
325 and associates if the items are required by an approved hazard review and acquired in
326 accordance with federal acquisition regulations:
327
- 328 i. Everyday clothing, such as long-sleeve shirts, long pants, street shoes, and normal
329 work shoes or boots;
330
- 331 ii. Weather-protection gear such as winter coats, jackets, gloves, parkas, rubber
332 boots, hats, raincoats, and ordinary sunglasses; and
333
- 334 iii. Protective skin creams, including sunscreen; insect repellent; and similar items.
335
- 336 (2) Replacement PPE shall be provided by the OUs at no cost to employees and associates
337 except when employees or associates have lost or intentionally damaged the PPE.
338
- 339 (3) NIST *may* use appropriated funds to purchase *individual-specific* PPE (see definition in
340 Section 7) for NIST employees under the following conditions:
341

⁶ This obligation only requires payment for PPE. It does not require payment for uniforms, caps, or other clothing worn solely to identify a person as an employee or associate. This obligation does not require payment for items worn to keep employees and associates clean for purposes unrelated to safety or health, e.g., coveralls, aprons, or other apparel when worn solely to prevent clothing or skin from becoming soiled, or clothing that is personal in nature and is worn as much off the job as on the job.

⁷ Employees covered under collective bargaining agreements may have negotiated payment for specific PPE. This suborder does not override those agreements.

(a) The individual-specific PPE must be special and not part of the ordinary and usual furnishings an employee may reasonably be expected to provide for himself;

(b) The provision of individual-specific PPE, as opposed to available generic alternatives to individual-specific PPE, must be for the benefit of the government; and

(c) The employee must be engaged in hazardous duty.

Any individual-specific PPE purchased by NIST for employees is and remains the property of the government, not the employees.

(4) NIST *may not* use appropriated funds to purchase individual-specific PPE for any individual who is not a NIST employee.

7. DEFINITIONS

a. Appropriated Funds – Funds made available to a Federal agency as a result of an act of Congress that permits the agency to incur obligations and to make payments out of the U.S. Department of the Treasury for *specified purposes*.

b. Employee – An individual employed by NIST who has been issued a NIST employee badge.⁸

c. Generic PPE – PPE not dedicated or designed solely for the use of a single individual, including, but not limited to, latex gloves; lab coats or jackets; non-prescription safety eyewear, including safety eyewear to be worn over prescription eyewear; disposable ear plugs; ear muffs; and disposable coveralls.

d. Individual-Specific PPE – PPE designed solely for the use of a single individual, including, but not limited to, prescription eyewear, custom-fitted safety shoes, and custom-designed fitted ear plugs.

e. Personal Protective Equipment (PPE) – Protective equipment used to reduce an individual's exposure to hazards when engineering and administrative controls are not feasible or effective on their own in reducing exposures to acceptable levels.

⁸ Technically, a "NIST employee" is defined as follows: The NIST Director or an individual who is (a) appointed in the civil service by an employee acting in an official capacity, (b) engaged in the performance of a Federal function under authority of law or an Executive act, and (c) subject to the supervision of the NIST Director or an individual named by paragraph (a) while engaged in the performance of the duties of his position (see 5 U.S. Code § 2105).

378 **8. ACRONYMS**

- 379 a. ANSI – American National Standards Institute
380
381 b. CFR – Code of Federal Regulations
382
383 c. OSH – Occupational Safety and Health
384
385 d. OSHE – Office of Safety, Health, and Environment
386
387 e. OU – Organizational Unit
388
389 f. PPE – Personal Protective Equipment
390
391 g. SDS – Safety Data Sheet
392
393

394 **9. ROLES AND RESPONSIBILITIES**

- 395 a. Employees and Associates Engaged in Activities in which They Are Required to, or
396 Voluntarily, Use PPE:
397

398 (1) Complete the training specified in Section 6c as assigned to them by their Official First-
399 Level Supervisors;

401 (2) Use, inspect, clean, maintain, and dispose of the PPE provided to them, or that they own,
402 in accordance with the requirements in Section 6a, as applicable, and their training; and
403

404 (3) Request additional training as duties change or as otherwise needed.
405

- 406 b. First-Level Supervisors of Employees and Associates Engaged in Activities in which They
407 Are Required to, or Voluntarily, Use PPE:
408

409 (1) Ensure that affected employees and associates they supervise are provided with, or own,
410 the PPE necessary to comply with the requirements of this and other applicable OSH
411 suborders, at no cost to affected employees and associates;
412

413 (2) Assign training to the affected employees and associates they supervise in accordance
414 with the requirements in Section 6c and do so when:
415

416 (a) Employees and associates enter on duty;
417

(b) Employees' or associates' duties change; and

(c) Special circumstances arise such as those indicated in Section 6c(3)(a);

(3) Ensure that the training specified in Sections 6c(1)(b) and 6c(3)(a) is documented and recorded in accordance with OU procedures; and

(4) Complete the training specified in Section 6c(2) for Official First-Level Supervisors.

c. OSHE PPE Program Manager:

(1) Ensure that training on the PPE program is available and meets the format, content, and documentation requirements of the Safety Education and Training suborder.

10. AUTHORITIES

a. First-Level Supervisors of Employees and Associates Engaged in Activities in which They Are Required to Use PPE:

(1) Approve, or disapprove, requests to purchase individual-specific PPE when the conditions specified in Section 6d(3) are satisfied.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

A. Revision History

448
449

Appendix A. Revision History

Revision No.	Approval Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	04/29/14	05/21/14	04/01/15	None – Initial document
1	11/13/15	11/13/15	11/13/15	<ul style="list-style-type: none">• Made suborder applicable to “associates”.• Revised Section 6d(1)(a) from “The following protective equipment is excepted from this requirement” to “OUs are not obligated to, but may, provide the following items to NIST employees and associates if the items are required by an approved hazard review and acquired in accordance with federal acquisition regulations..” This change allows OFPM to purchase, in accordance with the Federal Acquisition Regulation, sunscreen and similar items for workers whose jobs warrant them.

450
451
452

Safety Education and Training

NIST S 7101.23

Approval Date: 01/12/2016

Effective Date:¹ 01/12/2016

1. PURPOSE

The purpose of the Safety Education and Training suborder is to articulate NIST safety education and training requirements, roles, responsibilities, and authorities.

2. BACKGROUND

The safety education and training requirements, roles, responsibilities, and authorities in this suborder supersede those in NIST Administrative Manual Subchapter 12.01, Safety Operational System.

3. APPLICABILITY

a. This suborder applies to all NIST employees and covered associates.

b. This suborder covers:

(a) NIST General Safety Training;

(b) Training specified in NIST occupational safety and health (OSH) suborders;

(c) Training required by hazard reviews conducted in accordance with the requirements of the NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;

(d) Training required for Line Managers, Safety and Health Specialists, and OU/Division Safety Personnel (Full-Time and Collateral-Duty);

(e) Training required for Official First-Level Supervisors; and

¹ For revision history, see Appendix A.

- (f) Training specified by the Office of Safety, Health, and Environment (OSHE) based on special circumstances.

4. REFERENCES

- a. [Occupational Safety and Health Act of 1970, as amended, 29 United States Code \(U.S.C.\) § 651 et seq.](#);
- b. [Executive Order \(E.O.\) 12196](#), Occupational Safety and Health Programs for Federal Employees (1980);
- c. [29 CFR 1960](#), Basic Program Elements for Federal Employee Occupational Health and Safety Programs and Related Matters, Sections 54-59;
- d. Work and Worker Authorization Based on Hazard Reviews (“Hazard Review”) suborder;
- e. Safety Concerns suborder; and
- f. Incident Reporting and Investigation suborder.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews

6. REQUIREMENTS

NIST must meet the safety education and training requirements established by the Occupational Safety and Health Administration (OSHA) in [29 CFR 1960](#), Basic Program Elements for Federal Employee Occupational Health and Safety Programs and Related Matters, Standards 54-59. The following requirements achieve that objective.

- a. General Training Requirements

- (1) All employees and covered associates entering on duty other than Facility Users shall complete training provided by OSHE on general NIST safety policies and procedures, including employee rights and responsibilities (“NIST General Safety Training”).

b. Specific Training Requirements

(1) All employees and covered associates other than Facility Users, including employees and covered associates entering on duty, shall complete:

(a) The training specified in OSH suborders applicable to the work they are to conduct;² and

(b) The activity-specific training, to be provided by the OUs, required by hazard reviews applicable to the work they are to conduct.

(2) Line Managers, Safety and Health Specialists, and OU/Division Safety Personnel (Full-Time and Collateral-Duty) shall complete, in addition to the training in Section 6b(1), training provided by OSHE on:

(a) Section 19 of the OSH Act;

(b) Executive Order 12196;

(c) 29 CFR 1960; and

(d) [NIST O 710](#), including:

i. OSH-management-system requirements, roles, responsibilities, and authorities;

ii. The Management Observation suborder;

iii. The Hazard Review suborder;

iv. The Safety Education and Training suborder;

v. The Safety Rights and Responsibilities suborder;

vi. The Employee Reporting of Unsafe and Unhealthful Working Conditions suborder, including procedures for reporting and investigating employee allegations of reprisal for raising safety concerns;

² Training specified in an OSH suborder could be (a) training that is to be provided by OSHE, e.g., training on the associated OSH program (see definition of “Training on an OSH Program” in Section 7), or (b) training that is to be provided by the employee’s or covered associate’s OU, e.g., job-, activity-, or task-specific training.

- 115 vii. The Stop Work suborder; and
- 116
- 117 viii. The Incident Reporting and Investigation suborder.
- 118
- 119 (3) Official First-Level Supervisors shall complete, in addition to the training in Sections
- 120 6b(1) and 6(b)(2), introductory and specialized courses and materials that will enable
- 121 supervisors to recognize and eliminate, or reduce, OSH hazards in their working units
- 122 (see [29 CFR 1960.55](#)), including, at a minimum, training on the OSH programs
- 123 applicable to the work to be supervised.
- 124
- 125 (4) Affected employees and covered associates other than Facility Users shall complete
- 126 training specified by OSHE based on special circumstances, such as:
- 127
- 128 (a) Major changes in an OSH program;
- 129
- 130 (b) The identification of a material weakness in an OSH program;
- 131
- 132 (c) New regulatory requirements; or
- 133
- 134 (d) Regulatory notices of violation or similar actions.
- 135
- 136 c. Assignment of Training to Employees and Covered Associates Other than Facility Users
- 137
- 138 (1) Official first-level supervisors shall assign training to the employees and covered
- 139 associates they supervise, other than Facility Users, in accordance with the requirements
- 140 in Section 6b and they shall do so when:
- 141
- 142 (a) Such employees and covered associates enter on duty;
- 143
- 144 (b) Such employees' and covered associates' duties change with regard to safety;³ and
- 145
- 146 (c) Special circumstances arise such as those indicated in Section 6b(4).
- 147
- 148
- 149
- 150
- 151
- 152

³ For example, the employee or covered associate is to conduct work involving new OSH hazards, the employee is assigned to a line-management position for the first time, or the employee is assigned new collateral-safety duties.

d. Training for Facility Users

(1) Facility Users shall complete the following safety training prior to commencing work involving significant hazards, and any re-training and/or refresher training required by the User Facility:

(a) Training on pertinent User Facility safety policies and procedures;

(b) User-Facility-required courses; and

(c) Training on specific jobs and tasks to be performed, including, for example, SOPs and “how to” demonstrations.

e. Training Provided by OSHE

(1) Training provided by OSHE shall be made available in one or more of the following training formats:

(a) Instructor-led training;

(b) Demonstration or supervised practice; and

(c) Computer-based training, which may be used alone or in conjunction with instructor-led training and demonstration or supervised practice.

(2) Training provided by OSHE should include:

(a) Training objectives;

(b) Learning assessments, such as quizzes, checklists, or demonstrations, to demonstrate that training objectives have been met; and

(c) Evaluation tools, such as surveys, to obtain feedback at the end of the training for the purpose of improving the training.

f. Training Documentation⁴ and Recordkeeping

(1) Training specified in Section 6b that is to be provided by OSHE shall be documented and its completion by affected employees and covered associates shall be recorded in NIST’s electronic safety-training application, regardless of the training format.

⁴ See definition of “Training Documentation” in Section 7.

(2) Training specified in Sections 6b and 6d that is to be provided by the OUs⁵ shall be documented and its completion by affected employees and covered associates shall be recorded in accordance with OU procedures.⁶

g. Administration of NIST’s Electronic Safety-Training Application:

(1) Individuals shall be assigned by their OUs to assist in the administration of NIST’s electronic safety-training application.

7. DEFINITIONS

a. Documenting Training – The act of producing and maintaining training documentation (see definition of “Training Documentation”).

b. Facility User – Any individual who is permitted to use designated NIST facilities under a NIST Facility User Agreement. Designated NIST facilities include the NIST Center for Neutron Research and the Center for Nanoscale Science and Technology.

c. Line Managers – For the purposes of this suborder, the following or equivalent: NIST Director, Associate Directors, OU Directors and Deputy Directors, Division Chiefs, Deputy Division Chiefs, Group Leaders, and any Official Supervisors below the level of Group Leader.

d. NIST General Safety Training – Training provided by OSHE on general NIST safety policies and procedures.

e. Training on an OSH Program – Training provided by OSHE that includes:

(1) An overview of the requirements of an OSH program and associated roles and responsibilities;

(2) For OSH programs focused on OSH hazards, baseline knowledge on the identification, assessment, and control of those hazards; and

(3) Other relevant safety information.

⁵ This includes (a) training specified in OSH suborders that is to be provided by the OUs, and (b) activity-specific training required by hazard reviews.

⁶ OUs may elect to document and record activity-specific training required by hazard reviews in NIST’s electronic safety-training application.

- f. Official First-Level Supervisor (of Another Employee or of a Covered Associate) – The Rating Official on the performance plan of another employee or the supervisor of a covered associate.
- g. OU/Division Safety Personnel – Employees who have been designated to perform OSH-related duties in support of their OUs or Divisions on a full- or part-time basis.
- h. Recording Training – The act of creating a training record (see definition of “Training Record”).
- i. Safety and Health Specialist – A professional in occupational safety, industrial hygiene, health physics, or a related field.
- j. Training Documentation – Materials in electronic or hard-copy form that describe or embody the content of the training; any tools used to determine that training objectives have been met, *e.g.*, quizzes or checklists; and any evaluation tool(s) used to gather feedback at the end of the training, *e.g.*, surveys.
- k. Training Record – (a) A document evidencing the completion of training, including the subject of the training, the name of the individual who completed the training, the date on which the training was completed, and, when applicable, the name of the individual responsible for certifying that the training was completed; (b) any completed quizzes, checklists, or surveys.

8. ACRONYMS

- a. NIST – National Institute of Standards and Technology
- b. OSH – Occupational Safety and Health
- c. OSHA – Occupational Safety and Health Administration
- d. OSHE – Office of Safety, Health, and Environment
- e. OU – Organizational Unit

268 **9. ROLES AND RESPONSIBILITIES**

269 a. OU Directors:

270
271 (1) Ensure that procedures are implemented for documenting and recording the completion
272 by affected employees and covered associates other than Facility Users of:

273
274 (a) Training specified in OSH suborders that is to be provided by the OU; and

275
276 (b) Activity-specific training required by hazard reviews; and

277
278 (2) Ensure that individuals are designated to assist in the OU's administration of NIST's
279 electronic safety-training application.

280
281 b. Directors of NIST User Facilities:

282
283 (1) Ensure that Facility Users meet the training requirements detailed in Section 6d; and

284
285 (2) Ensure that procedures are implemented for documenting and recording the completion
286 by Facility Users of the training specified in Section 6d.

287
288 c. All Employees and Covered Associates Other than Facility Users Entering on Duty:

289
290 (1) Complete NIST General Safety Training;

291
292 d. All Employees and Covered Associates Other than Facility Users, Including Employees and
293 Covered Associates Entering on Duty:

294
295 (1) Complete the training in Section 6b assigned to them by their Official First-Level
296 Supervisors; and

297
298 (2) Request additional training as duties change or as otherwise needed.

299
300 e. Official First-Level Supervisors of Employees and Covered Associates Other than Facility
301 Users (in addition to the responsibilities of All Employees):

302
303 (1) Assign training to the employees and covered associates they supervise in accordance
304 with the requirements in Section 6b and do so when:

305
306 (a) Such employees and covered associates enter on duty;

(b) Such employees' and covered associates' duties change; and

(c) Special circumstances arise such as those indicated in Section 6b(4).

(2) Ensure that the following training is documented and its completion by affected employees and covered associates recorded in accordance with OU procedures:

(a) Training specified in OSH suborders that is to be provided by the OU; and

(b) Activity-specific training required by hazard reviews.

f. Chief Safety Officer:

(1) Ensure that an electronic safety-training application for documenting, assigning, and recording training is maintained by OSHE; and

(2) Ensure that the training specified in Sections 6a, 6b(2), and 6b(4) is available, meets the requirements in Section 6d, and is documented in NIST's electronic safety-training application.

g. OSHE Safety Program Managers:

(1) Articulate the training requirements for their assigned OSH programs in the associated OSH suborders; and

(2) When an OSH suborder indicates that training specified in the suborder is to be provided by OSHE, ensure that:

(a) The training is available;

(b) The training meets the requirements in Section 6d;

(c) The training is documented in NIST's electronic safety-training application; and

(d) The completion of the training by affected employees and covered associates is recorded in NIST's electronic safety training application, regardless of the training format.

h. Individuals Designated by their OU to Assist in the Administration of NIST's Electronic Safety-Training Application Within the OU:

(1) Carry out their assigned duties.

10. AUTHORITIES

a. Chief Safety Officer:

(1) Upon request and with suitable justification, approve training provided by one or more OUs as an alternative to training provided by OSHE; and

(2) Delegate the aforementioned authority to other OSHE employees.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

A. Revision History

Appendix A. Revision History

Revision No.	Approval Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	03/20/14	06/25/14	04/01/15	None – Initial document
1	01/12/16	01/12/16	01/12/16	<ul style="list-style-type: none">• Made suborder applicable to “covered associates”.• Revised Section 6 to establish separate training requirements for Facility Users versus other covered associates.• Added definition of “Facility Users” to Section 7.• Added responsibilities for the Directors of NIST User Facilities to Section 9.• Rationale for separate training requirements for Facility Users:<ul style="list-style-type: none">○ Short-term visits;○ Limited access to NIST site and facilities;○ No NIST IT accounts;○ Specifically-scoped activities; and○ Greater oversight of work by User Facility personnel.

INCIDENT REPORTING AND INVESTIGATION

NIST S 7101.24

Effective Date: 10/01/2013

Document Approval Date: 07/22/2013

1. PURPOSE

This suborder provides operational requirements regarding the reporting and investigation of work-related incidents through the NIST Incident Reporting and Investigation System (IRIS) and for the associated dissemination throughout the organization of incident information and lessons identified.

2. BACKGROUND

NIST management is committed to the safety of everyone who works for, works at, or visits NIST. As part of this commitment, NIST strives to prevent safety incidents by effectively managing risk in all of its activities. Essential to effectively managing risk is to learn as much as possible from incidents that have occurred and to take actions to prevent their recurrence. Success in this depends, in turn, on the prompt reporting of incidents and on the timely completion and use of the results of thorough incident investigations. Therefore, NIST shall report and investigate incidents in a thorough and timely manner, share incident reports and lessons identified effectively throughout the organization, and analyze incident data to identify systemic weaknesses in the NIST occupational safety and health (OSH) management system and to take actions to address those weaknesses.

3. APPLICABILITY

- a. The provisions of this suborder apply to the reporting and investigation of work-related incidents involving NIST employees, associates, and visitors at sites owned and operated by NIST, NIST employees and associates at other duty stations, and NIST employees and associates on official business away from these locations.

- b. The provisions of this suborder do not apply to incidents involving NIST associates working at sites owned and operated by NIST who are required to operate in accordance with their employers' NIST-accepted safety plan (see the NIST Contractor Safety Program).
- c. This suborder does not address the following topics:
 - (1) Emergency communications from staff members and first responders through Organizational Unit (OU) management and emergency communication channels, respectively, to NIST Director and Associate Directors, the Department of Commerce, and others pursuant to an emergency or potentially serious incident;
 - (2) Specific steps that employees and associates should take in the event they sustain work-related occupational injuries or illnesses; and
 - (3) Requirements associated with consequence management, *i.e.*, policies, procedures, and forms related to workers' compensation, automobile accidents, and personal property claims.

4. REFERENCES

- a. 29 Code of Federal Regulations (CFR) Part 1904, Recording and Reporting Occupational Injuries and Illness.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.23: Safety Education and Training; and
- b. NIST S 7101.02: Employee Reporting of Unsafe or Unhealthful Working Conditions.

6. REQUIREMENTS

- a. Establishment of OU Implementation Procedures

Each OU shall establish implementation procedures that include the following:

- (1) Reporting incidents that occurred.

- (a) Who staff must contact when they are involved in an incident; and

- (b) How staff must contact these individuals (*e.g.*, face-to-face, telephone, email, *etc.*).

(2) Initial Incident Reporting

- (a) Who is responsible for drafting the initial incident report;
- (b) What is the vetting process for the initial incident report; and
- (c) Who is responsible for submitting the initial incident report into the NIST Incident Reporting and Investigation System (IRIS).

(3) Incident Investigation and Reporting

- (a) Who is responsible for conducting the incident investigation;
 - (b) Who is responsible for drafting the incident investigation report;
 - (c) What is the vetting process for the incident investigation report; and
 - (d) Who is responsible for submitting the incident investigation report into IRIS;
- (4) Who is responsible for ensuring that the appropriate corrective actions have been implemented in a timely fashion and in such a way as to prevent the recurrence of the incident while not inadvertently introducing other hazards;
- (5) How lessons identified are shared, as appropriate, within the OU.
- (6) Who is responsible for acting as the OU IRIS Contact(s).

b. OU Initial Evaluation of Incidents Other than Immediate Notification Incidents

- (1) OUs shall evaluate an incident to determine if it can be immediately closed out, if additional time will be required to investigate the incident before the incident investigation report can be prepared and submitted, and if participation by OSHE and/or another entity in the incident investigation may be warranted or desired.
 - (a) For incidents that involve individuals and space from only one OU, that OU shall make this evaluation.
 - (b) For incidents involving multiple individuals and/or space from different OUs, the OU IRIS Contacts from all OUs involved shall collectively make this evaluation.

(c) For incidents where no individuals are involved (*e.g.*, flooding that occurred in a laboratory after hours or collapse of a bookshelf in an office when no one was present in the room), the OU responsible for the space in which the incident occurred shall make this evaluation.

(2) OUs may contact the OSHE Program Manager for Incident Reporting and Investigation for assistance with this evaluation.

c. Initial Incident Reporting

(1) Initial incident reports shall be submitted to IRIS, within 2 business days of line management being notified of an incident, if possible.

(2) For Immediate Notification incidents, OSHE, with participation from the OU(s) involved, shall submit an initial incident report.

(3) For incidents other than Immediate Notification incidents, initial incident reports shall be submitted by OUs as follows.

(a) For incidents that involve individuals and space from only one OU, that OU shall submit the initial incident report.

(b) For incidents involving multiple individuals and/or from different OUs, the OU IRIS Contacts from all OUs involved shall identify a lead OU to develop and submit a single initial incident report, with appropriate support from the other OU(s).

(c) For incidents where no individuals are involved (*e.g.*, flooding that occurred in a laboratory after hours or collapse of a bookshelf in an office when no one was present in the room), the OU responsible for the space in which the incident occurred shall submit the initial incident report.

(4) Initial incident reports shall contain the following information:

(a) Name and OU of the individual submitting the report;

(b) Type of incident (*e.g.*, exposure, illness, injury, near-miss, property damage, spill/release, other);

(c) Date and time of incident, if known;

- (d) Location of the incident;
 - (e) When OU line management was first notified of the incident;
 - (f) Who was involved in the incident (generic descriptions only, please do not provide names of individuals or specific positions);
 - (g) A brief description of injury or illness if one occurred;
 - (h) A brief description of any property damage;
 - (i) A brief description of the activity leading up to or taking place at the time of the incident;
 - (j) A brief description of the immediate impact of the incident;
 - (k) A brief description of any immediate measures taken to respond to the incident; and
 - (l) The OU responsible for conducting and reporting on the incident investigation (based on discussion among the OU IRIS contacts of the OUs involved).
- (5) Initial incident reports shall not contain information that could lead to the identity of individual(s) involved in the incident, some examples being:
- (a) Name of the individual;
 - (b) Birth date;
 - (c) Social security number; or
 - (d) Specific position description – should be kept generic, *i.e.*, “office personnel” as opposed to “Executive Assistant to the Chief Safety Officer”.

d. Incident Investigation

- (1) Incident investigations shall be conducted in accordance with established OU policies and procedures for investigating incidents.
- (2) OU(s) responsible for conducting incident investigations shall be as follows.

(a) For Immediate Notification incidents, OSHE, with participation from the OU(s) involved, shall conduct the incident investigation.

(b) For all other incidents:

- i. For incidents that involve individuals and space from only one OU, that OU shall conduct the incident investigation. Please note Section 6.d(2)(c) for additional clarification.
- ii. For incidents involving multiple individuals and/or space from different OUs, the OU IRIS Contacts from all OUs involved shall identify the lead OU to conduct the incident investigation, with appropriate support from the other OU(s). Please note Section 6.d(2)(c) for additional clarification.
- iii. For incidents where no individuals are involved (*e.g.*, flooding that occurred in a laboratory after hours or collapse of a bookshelf in an office when no one was present in the room), the OU responsible for the space in which the incident occurred shall conduct the incident investigation. Please note Section 6.d(2)(c) for additional clarification.

(c) If at any time it is determined that another OU is responsible for the activity in which the incident occurred, or for the apparent cause of the incident, the OU with responsibility for the activity or apparent cause will participate in or lead the investigation, or, if the investigation is already underway, the remainder of the investigation, as necessary and appropriate.

(3) When requested, OSHE shall provide assistance in conducting incident investigations.

(4) Some NIST OSH programs may require that certain OSHE staff members shall be a party to incident investigations involving specific OSH subject matter area, *e.g.*, the NIST Laser Safety Officer shall be a party to the investigation of incidents resulting from laser hazards.

e. Incident Investigation Reporting

(1) The OU responsible for conducting, or taking the lead in conducting, the incident investigation, shall submit the incident investigation report.

(a) If multiple OUs are involved in the investigation, each OU shall have the opportunity to comment on the incident investigation report prior to submission.

(2) Incident investigation reports shall be submitted within 20 business days of line management being notified of the incident, if possible.

(3) Incident investigation reports shall contain the following information:

- (a) All items listed under Section 6.c(4);
- (b) Name and OU of the individual submitting the report
- (c) Any causal factors;
- (d) The root cause;
- (e) Any corrective actions necessary; and
- (f) Any lessons identified for sharing with the broader NIST community.

f. Administration of IRIS

(1) Initial Incident Reports

- (a) The Program Manager for this safety program shall ensure that initial incident reports to be posted to IRIS do not contain information that can be used to identify specific individuals or that can be used with other sources to identify such individuals, see Section 6.c(5); and
- (b) The Program Manager for this safety program shall post initial incident reports to IRIS within 1 business day of submission, if possible.

(2) Incident Investigation Reports

- (a) The Program Manager for this safety program shall ensure that incident investigation reports to be posted to IRIS do not contain information that can be used to identify specific individuals or that can be used with other sources to identify such individuals, see Section 6.c(5); and
- (b) The Program Manager for this safety program should post the incident investigation report to IRIS within 2-3 business days of submission, if possible.

g. Training

(1) NIST-level training shall be provided to appropriate OU employees on the following:

- (a) Incident reporting requirements and responsibilities;
- (b) Incident investigation requirements and responsibilities;
- (c) Use of IRIS; and
- (d) Conduct of incident investigations.

(2) OU-level training shall be provided to all OU staff on the OU policies and procedures for reporting incidents;

(3) OU-level training shall be provided to appropriate OU staff on the OU policies and procedures for incident investigation and reporting.

(4) All training shall be documented and recorded in accordance with the requirements of the NIST Safety Education and Training suborder.

7. DEFINITIONS

- a. Accident – An incident that has given rise to a work-related injury, illness, or fatality, or to damage or loss of equipment or property.
- b. Condition – Any state, as found, whether or not resulting from an event, that may have adverse safety, health, environmental, or operational implications.
- c. Causal Factor – A condition or an event that results in an effect (anything that shapes or influences the outcome).
- d. Corrective Action – Action to eliminate the cause of a detected nonconformity or other undesirable situation.
- e. Event – For the purposes of this suborder, a real-time occurrence.
- f. Hazard – Source, situation, or act with a potential for harm in terms of human injury or ill health, adverse impact on the environment, damage or loss of equipment or property, or a combination of these.

- g. Illness (Work-Related) – Any abnormal condition or disorder, other than one resulting from a work-related injury, caused by continued or repeated exposure to environmental factors associated with employment, including acute and chronic illnesses or diseases that may be caused by inhalation, absorption, ingestion, or direct contact.
- h. Immediate Closeout – An incident where the causes, corrective actions, and lessons identified are clear at the time of the incident and the OU can submit both the initial incident report and the incident investigation report with little to no delay.
- i. Immediate Notification Incident – An incident that results in
 - (1) the death of an employee(s) or
 - (2) the in-patient hospitalization of three or more employees within thirty days of an incident.

Such incidents must be reported to OSHA within 8 hours of their occurrence or within 8 hours of a NIST employee being informed of their occurrence.

- j. Incident – A work-related event in which any of the following, individually or in combination, occurred or could have occurred: an injury or illness; an unauthorized spill or release of hazardous or regulated material to the environment; damage or loss of equipment or property. The “could have occurred” situation corresponds to “near misses”, defined below.
- k. Incident Investigation – The process of analyzing the events leading up to an incident, gaining an understanding of what caused it, identifying actions to prevent recurrence, and documenting the results in a written incident investigation report.
- l. Incident Investigation Report – A report that contains the items listed in Section 6.e(3).
- m. Incident Reporting – As described herein, the process of entering specific incident-related information, excluding information that can be used to identify specific individuals or that can be used with other sources to identify such individuals, into IRIS after an incident has occurred.
- n. Incident Reporting and Investigation System (IRIS) – A web-based IT application for reporting and disseminating incident information and the results of incident investigations, including lessons identified.
- o. Initial Incident Report – A report that contains the items listed in Section 6.c(4).

- p. Injury (Work Related) – Any wound or condition of the body caused by external force, including physical stress or strain that results from a work accident or from exposure in the work environment, e.g., amputation, bruise, burn, contusion, cut, fracture. The injury is identifiable as to time and place of occurrence and member or function of body affected, and is caused by a specific event or incident, or series of events or incidents, within a single day or work shift.
- q. Lessons Identified – Information resulting from an incident investigation that, if acted upon by an organization and the individuals therein, will reduce the probability of recurrence of that and similar incidents.
- r. Near Miss – Also known as a “near hit,” “near-accident,” or “close call,” an incident that did not result in any of the following, either individually or in combination, but had a plausible likelihood of doing so: a work-related injury or illness; a spill or release of hazardous or regulated material to the environment; damage or loss of equipment or property
- s. OU IRIS Contact – Individual identified by the OU Director as having the responsibility to coordinate efforts with other OUs when multiple OUs are involved in an incident through personnel, space, or both, to ensure that the reporting requirements of this program are met.
- t. OU Responsible for the Space – OU to which the space has been assigned by the Office of Facilities and Property Management.
- u. Property Damage – Loss or harm to property resulting from a safety-related incident.
- v. Root Cause – The cause of an incident that, if corrected, would prevent the recurrence of that and similar incidents. For example, in the case of a leak, the root cause could be management not ensuring that maintenance is effectively managed and controlled. This cause could have led to the use of improper seal material or missed preventive maintenance on a component, which ultimately led to the leak. In the case of a system misalignment, the root cause could be a problem in the training program, leading to a situation in which operators are not fully familiar with control room procedures and are willing to accept excessive distractions.
- w. Work Related – A condition wherein an injury, illness, or fatality was caused, contributed to, or significantly aggravated, or could have been, by an event or exposure at work or on official business away from work (see 29 CFR 1904.5).

8. ACRONYMS

- a. IRIS – Incident Reporting and Investigation System
- b. OSH – Occupational Safety and Health
- c. OSHA – Occupational Safety and Health Administration

9. RESPONSIBILITIES

- a. OU Directors are responsible for:
 - (1) Establishing OU implementation procedures and ensuring that those procedures are implemented;
 - (2) Ensuring the quality and timeliness of initial incident and incident investigation reports;
 - (3) Ensuring that applicable lessons identified are shared within their OU, as appropriate; and
 - (4) Ensuring that all-required follow-up actions are taken in accordance with the requirements of NIST Corrective and Preventive Actions Program.
- b. Supervisors are responsible for:
 - (1) Reporting all incidents as soon as practically possible to their management in accordance with OU policies and procedures;
 - (2) Ensuring that equipment and facilities involved in incidents are shut down if necessary and restored to use only after hazards have been mitigated;
 - (3) Preserving the scenes of incidents intact to the extent possible to facilitate incident investigations; and
 - (4) Supporting incident investigations as prescribed by their OU-level policies.
- c. Sponsors and Hosts are responsible for informing associates of the requirements to report incidents as soon as practically possible.
- d. OU IRIS Contacts are responsible for:

- (1) Coordinating efforts with other OUs when multiple OUs are involved in an incident through personnel, space, or both, to ensure that the reporting requirements of this program are met.

e. NIST Employees are responsible for:

- (1) Reporting (or having someone else report) all incidents immediately to their supervisor or sponsor; and
- (2) Providing complete and accurate information in support of incident investigations, as necessary and as prescribed by the OU-level policies.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

None

Biosafety

NIST S 7101.50

Document Approval Date: 03/18/2013

Effective Date: 04/01/2014

1. PURPOSE

The Biosafety suborder provides operational requirements and guidance to enable all NIST personnel to work safely with biohazardous materials.

2. BACKGROUND

None.

3. APPLICABILITY

a. The provisions of this suborder apply to all NIST facilities and to all NIST employees who work with biohazardous materials, with the exceptions noted in [NIST O 710](#), Occupational Safety and Health.

b. Breast milk that is collected for nursing purpose is excluded from the requirements of this suborder.

4. REFERENCES

a. National Institutes of Health, *NIH Guidelines for Research Involving Recombinant DNA Molecules*.

b. 42 CFR Part 73, Health and Human Services (HHS) *Possession, Use, and Transfer of Select Agents and Toxins*; Final Rule.

c. 7 CFR Part 331 and 9 CFR Part 121, Department of Agriculture (USDA), Agricultural Bioterrorism Protection Act of 2002; *Possession, Use, and Transfer of Biological Agents and Toxins*; Final Rule.

d. 29 CFR 1910.1030, *Bloodborne Pathogens*.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

a. NIST S 7101.51: Bloodborne Pathogens;

b. NIST S 7101.60: Chemical Management;

c. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;

d. NIST S 7101.22: Hazard Signage;

e. NIST S 7101.24: Incident Reporting and Investigation; and

f. NIST S 7101.23: Safety Education and Training

6. REQUIREMENTS

NIST S 7101.20: Work and Worker Authorization based on Hazard Reviews, requires the OUs to conduct hazard reviews of all activities prior to the initiation of those activities to ensure that proper precautions have been taken and proper practices are being followed to enable the safe conduct of the work by NIST employees. When activities involve the use of biohazardous materials, the OU must, as part of its overall hazard review process, submit a Biohazardous Materials Registration and Authorization Request to the BSO for review and approval. Many of the elements in this section pertain to the content of Biohazardous Materials Registration and Authorization Requests.

a. General Biosafety Requirements

(1) Registration and Authorization of the Use of Biohazardous Materials

(a) A Biohazardous Materials Registration and Authorization Request shall be completed and submitted to the BSO for review and approval for each activity that involves biohazardous materials.

(b) Research requiring BSL-3 and BSL-4 facilities is not currently permitted at NIST.

79 (2) Acquisition of Biohazardous Materials

- 80
- 81 (a) Acquisition of biohazardous materials from commercial vendors, other government
- 82 agencies, and/or academic institutions shall take place only after a Biohazardous
- 83 Materials Registration and Authorization Request has been approved by the BSO and
- 84 Division line management, and in the case of human cell lines, the IRB.
- 85

86 (3) Biosafety Risk Assessment and Assignment of RGs and BSLs

- 87
- 88 (a) A risk assessment shall be conducted by the researcher for each activity involving the
- 89 use of biohazardous materials. For factors that should be considered during the risk
- 90 assessment process, see Appendix B.
- 91

- 92 (b) Each biohazardous agent shall be assigned an RG and proposed BSL. This
- 93 information must be documented on the Biohazardous Materials Registration and
- 94 Approval Request.
- 95

- 96 i. RG assignments for specific agents may be found in various sources,
- 97 including Appendix B of the *NIH Guidelines* (Classification of Human
- 98 Etiologic Agents on the Basis of Hazard) and the American Biosafety
- 99 Association (ABSA) Risk Group Database. For selected examples of RG
- 100 assignments, see Appendix C.
- 101

- 102 ii. For descriptions of BSL classifications, see Appendix D.
- 103

- 104 (c) The BSO shall be available to assist researchers in performing risk assessments and
- 105 assigning RGs and BSLs.
- 106

107 (4) Certification of BSL 2 laboratories

- 108
- 109 (a) Laboratories shall be inspected and certified by the BSO to be BSL-2 compliant per
- 110 the BMBL guidelines prior to the start of biological experiments. For requirements,
- 111 refer to 8b.(1)(3), c(1)(2), and d(2) below.
- 112

113 (5) Inspection of Laboratories

- 114
- 115 (a) BSL 1 and BSL 2 laboratories shall be inspected annually in a manner to be
- 116 determined by the BSO. Inspections shall be announced, and an inspection checklist
- 117 shall be provided.
- 118

119 (6) Select Agents and Toxins

- 120
- 121 (a) The CSO, acting as the NIST Responsible Official in accordance with the
- 122 requirements of *Possession, Use, and Transfer of Select Agents and Toxins*, Final
- 123 Rule, must approve the acquisition of any select agent or toxin prior to that agent or
- 124 toxin being acquired. Furthermore, laboratories must be registered with and be
- 125 inspected by the CDC or the USDA prior to working with non-exempted select agents
- 126 and toxins. A list of the select agents and permissible toxin amounts can be found at
- 127 www.selectagents.gov.
- 128

129 (7) Recombinant DNA Experiments

- 130
- 131 (a) NIST researchers who receive funding from the NIH for rDNA research must adhere
- 132 to the NIH rDNA Guidelines.
- 133
- 134 (b) The acquisition and use of all rDNA materials shall be reviewed and approved by the
- 135 NBC.
- 136

137 (8) Animal Work

- 138
- 139 (a) Work involving animals may expose workers to zoonotic agents in a variety of ways
- 140 such as wound infections, inhalation of aerosols (e.g., dust from animal bedding), and
- 141 animal bites or scratches. Work with animals must be subjected to the hazard review
- 142 process in which appropriate controls are identified in accordance with the
- 143 requirements of the NIST Hazard Analysis and Control Suborder.
- 144
- 145 (b) Section VIII of BMBL provides agent summary statements for zoonotic agents.
- 146 Division Chiefs shall ensure that appropriate equipment and measures are utilized to
- 147 ensure that NIST personnel are protected during tasks involving animals.
- 148

149 b. Laboratory Practices

150 The following laboratory practices shall be observed by all employees.

151

152 (1) General Practices for All Biological Laboratories

- 153
- 154 (a) Access to the laboratory must be controlled in accordance with the requirements in
- 155 8.d.(1) and 8.d.(2) of this document;
- 156
- 157 (b) Laboratory personnel must wash their hands after working with potentially hazardous
- 158 biological materials and before leaving the laboratory;

- 159 (c) Eating, drinking, smoking, handling contact lenses, applying cosmetics, and storing
160 food for human consumption are not permitted in laboratory areas;
161
- 162 (d) Mouth pipetting is prohibited; mechanical pipetting devices must be used;
163
- 164 (e) Sharps precautions shall be observed in accordance to the NIST Bloodborne
165 Pathogens suborder;
166
- 167 (f) All procedures shall be designed to minimize the creation of splashes and/or aerosols;
168
- 169 (g) Work surfaces shall be decontaminated with appropriate disinfectant after completion
170 of work and after any spill or splash of potentially infectious materials;
171
- 172 (h) All potentially infectious biological materials shall be decontaminated using an
173 effective method prior to disposal. In addition:
174
- 175 i. Materials to be decontaminated outside of the immediate laboratory must be
176 placed in a durable, leak-proof container and secured for transport to the space
177 in which the decontamination will take place.
178
 - 179 ii. Materials to be removed from NIST for decontamination must be packed in
180 accordance with OSHE Environment Management Group's procedures, which
181 are in compliance with DOT (49 CFR Part 171-180) and OSHA (29 CFR Part
182 1910.1030) regulations.
183
- 184 (i) A sign incorporating the universal biohazard symbol must be posted at the entrance of
185 any BSL-1 or BSL-2 laboratory;
186
- 187 i. for BSL-2 laboratories, the sign must include the laboratory's BSL, the
188 supervisor's or laboratory contact's information, agents' information, and
189 instructions for entering and exiting the laboratory;
190
 - 191 ii. the signs must be removed when biohazardous materials are no longer
192 present; and
193
 - 194 iii. the signs must comply with the requirements of the NIST Hazard Signage
195 Suborder;
196

(j) The universal biohazard labels must be posted on refrigerators, freezers, and incubators where biohazardous materials are stored, and on containers that are used to transport biohazardous materials.

(k) All stored biohazardous materials must have labels containing the following information:

- i. Name of material;
- ii. Acquisition or production date; and
- iii. Initials of user.

For storage containers that are too small to capture all the labeling requirements listed above, a numbering system documented with the corresponding information is acceptable.

(l) All biohazardous materials must be inventoried for storage.¹

(2) Special Additional Practices for BSL 1 Laboratories

(a) No special additional practices are required.

(3) Special Additional Practices for BSL 2 Laboratories

(a) All persons entering the laboratory must be advised of the potential hazards using general and specific NIST hazard signs;

(b) Laboratory personnel must be provided medical surveillance, as needed, and offered available immunizations for agents handled or potentially present in the laboratory;

(c) A laboratory-specific biosafety manual must be prepared (using, e.g., the NIST Requirements found in this document as a template), adopted as policy, and made available in hard copy in the laboratory;

¹ The on-line biohazardous materials database will have the capability of meeting this requirement. For biohazardous materials that either exhibit hazardous chemical properties or mixed with other hazardous chemicals, the hazardous chemicals shall be registered separately in the Chemical Inventory System (CISPro) in accordance with the requirement of the NIST Chemical Management suborder.

- (d) Proficiency in standard and special microbiological practices must be demonstrated by laboratory personnel before they are authorized to work with BSL-2 agents;
- (e) Potentially infectious materials must be placed in a durable, leak proof container during collection, handling, processing, storage, or transport within a facility;
- (f) Laboratory equipment should be routinely decontaminated, especially after spills, splashes, or other potential contamination;
- (g) Equipment must be decontaminated by the owner before repair, maintenance, or removal from the laboratory;
- (h) Spills involving infectious materials must be contained, decontaminated, and cleaned up by staff properly trained and equipped to work with infectious materials; and
- (i) For incidents that result or could have resulted in exposure to infectious materials:
 - i. a report must be made to the first-level supervisor or group leader and a report must be filed to the NIST Incident Reporting and Investigation System (IRIS) in accordance to the requirements of the NIST Incident Reporting and Investigation Suborder;
 - ii. medical evaluation, surveillance, and treatment should be provided; and
 - iii. appropriate records shall be maintained.

c. Safety Equipment

Appropriate containment devices and PPE shall be available in all biological laboratories.

(1) Containment Devices

- (a) Containment devices such as Biological Safety Cabinets (BSCs) are not required in BSL-1 laboratories.
- (b) Properly maintained BSCs shall be used in BSL-2 laboratories whenever procedures with the potential for creating aerosols or splashes are performed. Such procedures may include, but are not limited to, pipetting, centrifuging, vortexing, homogenizing, and sonicating. Activities involving both biohazardous materials and hazardous volatile chemicals could be conducted in specific types of BSC or properly maintained fume hoods after a thorough risk assessment has been conducted by the

researcher and approved by the BSO. A centrifuge with sealed rotor or sealed safety buckets shall also be made available, if needed.

(c) BSCs shall be located away from doors and from high traffic areas in the laboratory to reduce disruption of air flow in the BSCs.

(d) BSCs must be tested and certified annually or after installation, repair, or relocation. The certification must be performed by vendors certified by the National Sanitation Foundation.

(e) For recommended practices for working in a BSC, see Appendix E.

(2) Personal Protective Equipment (PPE)

(a) Once a biological and/or procedural hazard has been identified, the required PPE shall be determined as part of the hazard review process. Minimum PPE for working with biohazardous materials includes gloves, protective eyewear, laboratory coats, closed-toe and closed-back shoes, and long pants.

(b) Area-specific PPE requirements shall be established and posted on the laboratory entrance in accordance with NIST Hazard Signage Suborder.

(c) In BSL-2 laboratories, when it is anticipated that potentially infectious biological materials could splash or splatter during work performed outside a BSC, appropriate face protection shall be worn. Such protection would include, but is not limited to, goggles, side-shielded safety glasses, and full-face shields. Bench-top splash shields can be used instead of full-face shields.

(d) Long-sleeved lab coats or gowns shall be worn to protect skin and personal clothing from contamination. Protective clothing shall not be worn outside of laboratory. Reusable lab coats or gowns shall be laundered on-site or by a laundering service at least once a month or whenever gross contamination occurs. Personnel shall not launder lab coats or gowns at home. Disposable gowns shall be used when on-site laundering service is not available. Disposable gowns shall be replaced at least once a month or whenever gross contamination occurs.

(e) Gloves must be worn when handling biohazardous materials. Use of standard nitrile or powder-free latex gloves is considered adequate for handling most biohazardous materials. Non-latex glove alternatives shall be made available to researchers who are allergic to latex gloves. Gloves shall be considered single use only and disposed

- 311 of at the conclusion of the task as infectious/medical waste. Hands shall be washed
312 immediately after the removal of gloves at the conclusion of the task.
313
- 314 (f) When significant splash and splatter are anticipated, disposable shoe-covers/booties
315 shall be worn. Prior to exiting the laboratory, these must be removed and be disposed
316 of as infectious waste.
317
- 318 (g) If gross contamination occurs, PPE shall be removed immediately and replaced. PPE
319 shall be removed and be disposed of with other biohazardous waste before exiting the
320 laboratory.
321
- 322 d. Facilities
323
- 324 (1) BSL-1 Laboratories
325
- 326 (a) Laboratories should have lockable doors for access control.
327
- 328 (b) Laboratories must have a sink for hand washing.
329
- 330 (c) The laboratory should be designed so that it can be easily cleaned. Carpet and rugs in
331 laboratories are not appropriate.
332
- 333 (d) Laboratory furniture must be capable of supporting anticipated loads and uses.
334 Spaces between benches, cabinets, and equipment should be accessible for cleaning.
335
- 336 (e) Bench tops must be impervious to water and resistant to heat, organic solvents, acids,
337 alkalis, and other chemicals.
338
- 339 (f) Chairs used in laboratory work must be covered with a non-porous material that can
340 be easily cleaned and decontaminated with appropriate disinfectant.
341
- 342 (2) BSL-2 Laboratories
343
- 344 (a) Laboratory doors should be self-closing and have locks. Only authorized personnel
345 shall have access to the laboratories.
346
- 347 (b) Laboratories must have a sink for hand washing. The sink may be manual, hands-
348 free, or automatic. It should be located near the exit door.
349

- (c) The laboratory should be designed so that it can be easily cleaned. Carpet and rugs in laboratories are not allowed.
- (d) Laboratory furniture must be capable of supporting anticipated loads and uses.
- (e) Spaces between benches, cabinets, and equipment should be accessible for cleaning.
- (f) Bench tops must be impervious to water and resistant to heat, organic solvents, acids, alkalis, and other chemicals.
- (g) Chairs used in laboratory work must be covered with a non-porous material that can be easily cleaned and decontaminated with appropriate disinfectant.
- (h) Biosafety cabinets, where applicable, should be installed so that fluctuations of the room air supply and exhaust do not interfere with proper operations. BSCs should be located away from doors, heavy-traffic areas, and other possible airflow disruptions.
- (i) Vacuum lines should be protected with an inline HEPA filter and liquid disinfectant traps.
- (j) An eyewash station must be available in the laboratory or be in accessible locations that require no more than 10 seconds to reach. The eyewash station shall be located on the same level as the hazard and the path of travel shall be free of obstructions that may inhibit the immediate use of the equipment.
- (k) A method for decontaminating all biohazardous wastes should be available in divisional laboratories (e.g., autoclave, chemical disinfection, incineration, or other validated decontamination method).

e. Disinfectants, Decontamination, and Biohazardous Spill Clean-up

Appropriate decontamination supplies such as disinfectants, absorbent pads/wipes, biohazardous waste bags, gloves, and tongs or forceps to pick up broken glass shall be available in all biological laboratories.

(1) Disinfectants

- (a) Chemical disinfectants that are registered as EPA tuberculocidal disinfectants are suitable for surface decontamination, equipment decontamination, spill cleanup, and liquid waste disinfection.

(b) Commonly used chemical disinfectants such as 70% ethanol solution, freshly prepared 10% bleach solution, and Cavicide are acceptable for use in biological laboratories.

(c) A 10% bleach solution or an equally effective formulation shall be used for surface decontamination after working with human specimens and cleaning up spills involving human specimens. Each bleach solution container must be labeled with either a made-on date or an expiration date, which is 24 hours after the day the solution was made.² Check the production date on the commercial bleach container before use.

(2) Decontamination

(a) All bench surfaces and equipment used in experiments shall be decontaminated when work is completed.

(b) Prior to decontaminating contaminated equipment, see the user's manual for compatible disinfectants.

(3) Biohazardous Spill Cleanup

(a) For recommended procedures for cleaning up spills of biohazardous materials, see Appendix F.

f. Biohazardous Waste Management

(1) On-Site Waste Treatment

(a) Steam sterilization (autoclaving) is an acceptable method for treating solid and liquid biohazardous waste generated on site at NIST. Only autoclavable biohazardous waste bags shall be used for autoclaving. For onsite autoclaving procedures, see Appendix G.

(b) Chemical disinfection

i. Chemical disinfection is an alternative treatment option for liquid biohazardous waste.

² When bleach and water are mixed to create a disinfecting solution, the solution begins to lose its disinfecting properties after 24 hours. Furthermore, commercial bleach begins to degrade approximately 20% each year after being stored for six months at temperatures between 10 and 21 degrees Celsius (50 and 70 degrees Fahrenheit).

- 426
- 427 ii. Chemical disinfectants that are registered as EPA tuberculocidal disinfectants
- 428 are acceptable for liquid biohazardous waste disinfection. A freshly prepared
- 429 10% bleach solution is an effective disinfectant, particularly for human
- 430 specimens. A minimum contact time of 20 minutes is recommended for a
- 431 10% bleach solution disinfection.
- 432
- 433 iii. Properly disinfected liquid biohazardous waste (with no hazardous chemicals)
- 434 can be disposed of down the drain.
- 435
- 436 (c) Solid and liquid hazardous microbiological and molecular waste, human specimens,
- 437 and tissue culture waste must be autoclaved before disposal. As an alternative, liquid
- 438 biohazardous waste can be disinfected by chemical disinfectants.
- 439
- 440 (d) Pipets and pipet tips that have come in contact with risk groups 2 and human
- 441 specimens should be placed in a pipet container, and when three-quarters full, the
- 442 container should be autoclaved before disposal. Alternatively, contaminated pipets
- 443 and pipet tips can be chemically disinfected. Chemically disinfected pipets/pipet tips
- 444 can then be placed in a biohazard waste receptacle.
- 445
- 446 (e) Disposable gloves, gauze, parafilms, vials, test tubes, and other laboratory supplies
- 447 that have come in contact with risk groups 2 agents and human specimens must be
- 448 autoclaved before disposal.
- 449
- 450 (f) Potentially infectious materials (risk group 2 agents, biological toxins, and human
- 451 specimens) and associated laboratory materials that have not been disinfected can be
- 452 disposed directly into the biohazard waste receptacles, as long as the materials are
- 453 contained and the receptacles are covered with lids. Lids are not required for
- 454 biohazard waste receptacles such as cardboard waste boxes that contain disinfected or
- 455 properly contained (e.g., in closed pipet containers or closed waste bags) infectious
- 456 materials.
- 457
- 458 (g) Laboratory supplies (non-sharps) that have come in contact with only risk group 1
- 459 agents can be disposed of in regular trash.
- 460
- 461 (2) Off-site Waste Treatment and Disposal
- 462
- 463 (a) For NIST Gaithersburg and Boulder researchers without access to an autoclave, an
- 464 off-site biohazardous waste treatment and disposal option is available through OSHE.
- 465 All solid and liquid biohazardous waste shall be properly contained before disposal

- 466 into a red biohazardous waste bag. When the red biohazard bag is three-quarters full,
467 it should be tied off and placed in a biohazardous waste cardboard box, which should
468 then be taped closed. The bags and boxes should be handled only when wearing
469 gloves and lab coat. Contact OSHE for pick-up of the biohazardous waste cardboard
470 boxes.
- 471
- 472 (b) All sharps (e.g., needles, syringes with attached needles, capillary tubes, slides and
473 cover slips, scalpel blades, razor blades, and broken contaminated glassware) must be
474 disposed in a rigid, puncture-resistant, and leak-proof sharps container with a
475 universal biohazard label. When the container is three-quarters full, contact OSHE
476 for hazardous waste pick up.
- 477
- 478 g. Transportation and Shipping of Biohazardous Materials
- 479
- 480 (1) Intra-Campus and Local Transfers of Biohazardous Materials
- 481
- 482 (a) Biohazardous materials to be transferred intra-campus should be placed in a closable
483 primary container. Absorbent material should be placed around the primary
484 container. The primary container and absorbent materials are then placed into a
485 closable secondary container. A universal biohazard label shall be placed on the
486 secondary container. The secondary container should be disinfected routinely.
- 487
- 488 (2) Shipping of Biohazardous Materials
- 489
- 490 (a) The International Air Transportation Association's (IATA) Dangerous Goods
491 Regulations (DGR) govern all international and domestic air transport of
492 biohazardous materials. IATA classifies biohazardous materials into Category A
493 Infectious Substances, Category B Biological Substances, and Exempt Human
494 Specimens. These categories have different packaging and labeling requirements.
495 All personnel involved with the shipping of Category A infectious substances are
496 required to receive training on the applicable requirement. Contact the BSO for
497 assistance in shipping biohazardous materials out of NIST.
- 498
- 499 h. Importation of Etiologic Agents
- 500
- 501 (1) In general, a permit from the United States Public Health Service Division of Quarantine
502 is required for the importation of any infectious agent known to cause disease in humans.
503 Contact the BSO prior to requesting such a permit.
- 504
- 505 i. Emergency Response

(1) All BSL 2 laboratories shall establish emergency response procedures based on the biohazardous materials used. Notify OSHE personnel when a spill or exposure to a biohazardous agent occurs outside of primary containment such as the BSC and report the incident to IRIS.

(2) Refer to Appendix H for a limited list of emergency response procedure examples.

j. Medical Surveillance

(1) Occupational Health and Immunizations

(a) The NIST Health Unit will provide immunization consultations and occupational health support for incidents involving exposure to biological hazards.

(2) Injuries and Illnesses Involving Biohazardous Materials

(a) Injuries and illnesses resulting from exposure to a hazardous biological agent shall be reported using the NIST Incident Reporting and Investigation System.

k. Decommissioning of Biological Laboratories

(1) Biological laboratories shall be decommissioned in accordance with the following procedures when biological work in them is terminated:

(a) All biohazardous materials must be removed from the laboratory by disposing of them according to the requirements of this suborder, shipping them to another facility following approved shipping regulations, or transferring them with proper documentation to another NIST responsible party.

(b) All biohazardous waste shall be properly decontaminated and disposed of in accordance with the requirements of this suborder.

(c) All equipment that has come in contact with the biohazardous materials shall be properly decontaminated.

(d) All bench-tops or other work surfaces where biohazardous materials were manipulated must be wiped down with an approved disinfectant.

(e) All BSCs must be properly decontaminated.

(f) All other hazards in the laboratory shall be handled in accordance with other NIST OSH suborders.

(g) The steps taken to decommission the laboratory shall be documented by the OU responsible for the laboratory and reviewed and approved by the BSO.

l. Training

(1) Training shall be provided, documented, and recorded in accordance with the requirements of the NIST Safety Education and Training Suborder.

(2) BSL 2 laboratory supervisors shall complete a one-time supervisory biosafety training course developed by OSHE. Prior participation and completion of the NIST Biosafety and Biocontainment Training BSL 2 Supervisory Training satisfies this requirement.

(3) All new employees who will be working with biohazardous materials shall complete an OSHE-instructor-led biosafety training course prior to working with biohazardous materials.

(4) All current employees who will be working with biohazardous materials for the first time shall complete an OSHE-instructor-led biosafety training course prior to working with biohazardous materials. Prior participation and completion of the NIST Biosafety Basics and Compliance Training satisfies this requirement.

(5) All employees who work with biohazardous materials shall complete an OSHE-developed on-line biosafety training refresher course every two years.

(6) All employees who work with biohazardous materials at BSL 2 shall complete an OSHE-provided one-time, hands-on biosafety techniques training course. After completing the training and obtaining concurrence from the BSO, parties designated by their OUs as responsible for the safety of activities in laboratories in which such work is conducted may provide this training to other laboratory personnel.

(7) All employees who ship Category A infectious substances shall receive applicable DOT and IATA training.

m. Biosecurity

(1) Biosecurity safeguards that may be used at NIST include, but are not limited to, risk and threat assessments, facility security plans, laboratory access policies, and biohazardous material inventories.

(2) Suspected thefts of RG 2 agents shall be reported to OSHE and local law enforcement officials immediately.

7. DEFINITIONS

a. Autoclave – Equipment with a chamber used to sterilize items by applying wet heat (i.e., high-pressure steam) at temperatures above the normal boiling point of water and pressures above normal atmospheric pressure.

b. Biohazard – A biological material or agent that presents potential risk to the health of humans or other organisms either directly through infection or indirectly through damage to the environment. Biohazards include, but are not limited to, bacteria; fungi; viruses; parasites; rickettsia; biological toxins; prions; non-human mammalian cell lines and tissues; human specimens such as human blood, serum, plasma, blood products, primary and continuous human cell lines, unfixed human tissues, fecal materials, semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, pericardial fluid, peritoneal fluid, amniotic fluid, saliva, tears, sweat, breast milk, and urine; and recombinant DNA materials such as inserts or vectors that are known to express toxins, oncogenes, and/or virulent factors.

Non-toxic proteins and commercially available enzymes, cell culture medium and supplements, reagents such as monoclonal antibodies, and random DNA base pairs are not considered biohazards.

c. Biohazardous – Describes a biological agent/material with the risk of posing a potential hazard.

d. Biohazardous Material – See definition of *biohazard*.

e. Biohazardous Materials Registration and Authorization Request – A NIST form submitted by the Organizational Unit (OU) to the Biosafety Officer (BSO) for review and approval as part of the OU hazard review process for activities that involve the use of biohazardous materials.

f. Biohazardous Waste – Waste that includes, but is not limited to, discarded microbiological cultures, stocks and all associated materials, discarded human specimens and all associated

materials, discarded tissue cultures and stocks, discarded live and attenuated vaccines, discarded molecular waste, and contaminated sharps.

- g. Biological Agent – A biological organism or material that is often directly responsible for producing an effect (e.g., disease). Agent examples include bacterium, fungus, parasite, Rickettsia, virus, proteinacious infectious particle (prion), or biological toxin.
- h. Biological Materials – A broad range of microbiological agents, recombinant DNA materials, non-human mammalian cell lines and tissues, human blood and blood products, and other materials of human, animal, and plant origins.
- i. Biosafety Cabinet or Biological Safety Cabinet (BSC) – A cabinet with built-in high-efficiency particulate air (HEPA) filters that provides personnel, environmental, and sample protection when appropriate practices and procedures are followed. When combined with appropriate microbiological techniques, the three classes of BSC provide different levels of protection:
 - (1) Class I BSCs, which are rarely used in biological laboratories, provide protection to personnel and the environment only, not the sample;
 - (2) Class II BSCs, which are the most commonly used BSCs at NIST at the current time, provide personnel, environmental, and sample protection; and
 - (3) Class III BSCs, which are used when working with agents in Risk Groups 3 and 4, provides maximum personnel, environmental, and sample protection.
- j. Biosafety Level (BSL) – Also known as a level of containment, a combination of standard laboratory practices and techniques, safety equipment, and facility design specifications for containing biohazardous materials. The CDC distinguishes the following four levels:
 - (1) Biosafety Level 1 (BSL 1), for working with well-characterized agents not consistently known to cause disease in healthy adult;
 - (2) Biosafety Level 2 (BSL 2), for working with agents associated with human disease for which the routes of transmission include percutaneous injury, ingestion, and mucous membrane exposure;
 - (3) Biosafety Level 3 (BSL 3), for working with indigenous or exotic agents that may cause serious or potentially lethal disease as a result of exposure by the inhalation route; and

(4) Biosafety Level 4 (BSL 4), for working with dangerous and exotic agents that may pose a high individual risk of aerosol-transmitted laboratory infections that are frequently fatal, for which there are no vaccines or treatments.

k. Biosafety Officer (BSO) – Also known as the Biological Safety Officer, a person appointed by the Chief Safety Officer as the OSHE Safety Program Manager for the NIST Biosafety Program.

l. Biosecurity – A set of preventive measures designed to reduce the risk of loss and/or intentional removal (theft) of valuable and/or regulated biohazardous materials.

m. Decontamination – The process of reducing or inactivating biohazardous contaminants or components to an acceptable level to reduce or eliminate the possibility of transmission of pathogens to undesired hosts such as laboratory workers, the general public, and other organisms in the environment.

n. Disinfectant – A chemical germicide agent that is applied to inanimate objects to kill microbes, but is not capable of killing endospores, some viruses, or mycobacterium. Disinfectants are typically chemical germicides. Common chemical disinfectants include 10% diluted household bleach and 70% ethanol.

o. Disinfection – A process of eliminating nearly all recognized pathogenic microorganisms but not necessarily all microbial forms (e.g., bacterial spores) from inanimate objects (e.g., work surfaces, equipment).

p. Etiologic – An adjective that means disease-causing.

q. Fixed – A biological material that has been chemically treated for preservation. Certain fixatives such as paraformaldehyde or glutaraldehyde are capable of rendering the biological materials inactive.

r. High-Efficiency Particulate Air (HEPA) Filter – A medium composed of pleated borosilicate fiber sheets capable of trapping at least 99.97% of airborne mono-dispersed particles of 0.3 micrometers (µm) in diameter.

s. Human Specimens – Human blood, serum, plasma, products made from blood, primary and continuous cell lines, tissues, fecal materials, semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, pericardial fluid, peritoneal fluid, amniotic fluid, saliva, tears, sweat, breast milk, and urine.

- t. Infectious Substances – Materials known to be, or suspected to contain, an animal or human pathogen, and that must be transported according to Department of Transportation (DOT) and the International Air Transport Association (IATA) shipping guidelines. There are two categories of infectious substances:
- (1) Category A – Materials capable of causing permanent disability or a life threatening or fatal disease in humans or animals, and that must be transported according to DOT and IATA shipping guidelines.
 - (2) Category B – Infectious materials that do not fall within Category A but still must be transported following DOT and IATA shipping guidelines.
- u. Medical or Infectious Waste – Infectious human or animal waste generated or produced as a result of research, a medical diagnosis, treatment, or immunization.
- v. Recombinant DNA (rDNA) – The NIH rDNA Guidelines define rDNA as 1) molecules that are constructed outside living cells by joining natural or synthetic DNA segments to DNA molecules that can replicate in a living cell, and 2) molecules that result from the replication of molecules described in 1).
- w. Risk Group (RG) – A system adopted by the CDC and NIH that classifies biohazardous agents by the health risk they present to individuals and surrounding communities. The system comprises risk groups numbered 1 through 4, with higher numbers corresponding to higher risks. More specifically:
- (1) Risk Group 1 (RG 1) agents are not associated with disease in healthy adult humans;
 - (2) Risk Group 2 (RG 2) agents are associated with human diseases that are rarely serious, and often have preventive or therapeutic interventions available;
 - (3) Risk Group 3 (RG 3) agents are associated with serious or lethal human disease for which preventive or therapeutic interventions may be available (high individual risk but low community risk); and
 - (4) Risk Group 4 (RG 4) agents are likely to cause serious or lethal human disease for which preventive or therapeutic interventions are not usually available (high individual risk and high community risk).
- Agents not listed in Risk Groups 2, 3, or 4 are not implicitly classified in RG 1. Refer to Appendix B for relationship between RG and BSL.

- x. Select Agents and Toxins – Specific pathogenic agents and toxins strictly regulated by the CDC and USDA (i.e., under 7 CFR 331, 9 CFR 121, and 42 CFR 73) because they may be used as agents of mass destruction or pose a severe threat to human, animal, and plant health; or they are specific genetic elements, recombinant nucleic acids, or recombinant organisms that are related to the list of select agents and toxins as described in the regulations.
- y. Sharp – An object that can penetrate the skin. A sharp is often a tool, device, or material that typically has a sharp edge or point such as a needle, scalpel, blade, razor, broken glass, broken capillary tube, or an exposed end of a wire.
- z. Standard Microbiological Practices - Administrative controls listed as BSL containment practices in BMBL and the *NIH Guidelines* to protect workers and the environment.
- aa. Sterilization - The process of destroying all living microorganisms and viruses on an object. Common sterilization methods include autoclaving and incineration.

8. ACRONYMS

- a. APHIS – Animal and Plant Health Inspection Service
- b. BMBL – Biosafety in Microbiological and Biomedical Laboratories
- c. BSC – Biological Safety Cabinet or Biosafety Cabinet
- d. BSL – Biosafety Level
- e. BSO – Biological Safety Officer
- f. CDC – Centers for Disease Control and Prevention
- g. CFR – Code of Federal Regulations
- h. DNA – Deoxyribonucleic acid
- i. DOT – Department of Transportation
- j. HHS – Health and Human Services
- k. IATA – International Air Transport Association

- l. IRB – Institutional Review Board
- m. IRIS – Incident Reporting and Investigation System
- n. NBC – NIST Biosafety Committee
- o. NIH – National Institutes of Health
- p. OSHA – Occupational Safety and Health Administration
- q. PPE – Personal Protective Equipment
- r. rDNA – Recombinant DNA
- s. RG – Risk Group
- t. RO – Responsible Official
- u. USDA – United States Department of Agriculture

9. RESPONSIBILITIES

- a. The Chief Safety Officer is responsible for:

- (1) Appointing an OSHE staff member to serve as the NIST Biological Safety Officer (BSO) to carry out the responsibilities for this position delineated below;
- (2) Serving as the Responsible Official in accordance with the requirements of *Possession, Use, and Transfer of Select Agents and Toxins*, Final Rule.

- b. Division Chiefs (or Equivalents) are responsible for:

- (1) Ensuring that staff have adequate supplementary instructions and guidance regarding specific practices and procedures unique to the work being conducted in their organization's laboratories; and
- (2) Ensuring that BSL-2 laboratories in their organizations have specific biosafety manuals.

NOTE: Some NIST OUs do not have Division Chiefs; these OUs should designate other individuals to carry out these responsibilities.

c. Employees are responsible for:

- (1) Completing and submitting Biohazardous Materials Registration and Authorization Requests to OSHE; as part of the OU hazard review process for activities that involve the use of biohazardous materials.

d. Biological Safety Officer (BSO) is responsible for:

- (1) Pursuant to discussions with OU personnel as appropriate, reviewing and approving Biohazardous Materials Registration and Authorization Requests as part of the OU hazard review process for activities that involve the use of biohazardous materials, or, in the case of activities that involve rDNA, present significant new or unique risks, or involve the non-exempted use of select agents or toxins, referring those requests to the NIST Biosafety Committee for review and approval;
- (2) Performing annual inspections of BSL-1 and BSL-2 laboratories;
- (3) Reviewing plans for new BSL-2 laboratories and renovations and providing recommendations on ventilation and design; and
- (4) Assisting the CSO in serving as the Responsible Official in accordance with the requirements of *Possession, Use, and Transfer of Select Agents and Toxins*, Final Rule.

e. NIST Biosafety Committee is responsible for:

- (1) Advising the CSO on the status of the NIST Biosafety Program;
- (2) Reviewing and approving Biohazardous Materials Registration and Authorization Requests not approved by the BSO, at the request of the submitting OU; and
- (3) Reviewing and approving Biohazardous Materials Registration and Authorization Requests for activities that involve rDNA, present significant new or unique risks, or involve the non-exempted use of select agents or toxins.

f. Chief Facilities Management Officer is responsible for:

- (1) Implementing an effective and integrated NIST pest management program.

862
863
864
865 **10. AUTHORITIES**

866 There are no authorities specific to this suborder alone.
867

868
869 **11. DIRECTIVE OWNER**

870 Chief Safety Officer
871

872
873 **12. APPENDICES**

874 a. Appendix A. Revision History
875

876 b. Appendix B. Risk Assessment Factors
877

878 c. Appendix C. Risk Groups: Selected Examples
879

880 d. Appendix D. Biosafety Level Classifications
881

882 e. Appendix E. Recommended Practices for Working in Biological Safety Cabinets
883

884 f. Appendix F. Recommended Procedures for Cleaning Up Spills of Biohazardous Materials
885

886 g. Appendix G. Recommended Procedures for Autoclaving Biohazardous Materials
887

888 h. Appendix H. Emergency Response Procedures - Examples
889
890

891
892

Appendix A. Revision History

Revision	Date	Responsible Person	Description of Change
None	03/18/13	Wing Wong	None – initial document.

893
894

Appendix B: Risk Assessment Factors

- (1) Risk groups correlate with but do not necessarily equate to biosafety levels. For example:
 - (a) When a significant amount of aerosol is generated from working with RG-1 agents, the aerosol-generating step should be conducted in a BSL-2 containment device such as a biological safety cabinet.
 - (b) Work with a known RG-3 agent such as the Human Immunodeficiency Virus can be conducted in a BSL-2 laboratory, depending on the amount of the agent being used.
- (2) Risk assessment determines the degree of correlation between an agent's risk group classification and biosafety level. Factors to be considered during the risk assessment process include, but are not limited to:
 - (a) Material pathogenicity;
 - (b) Route of transmission;
 - (c) Infectious dose;
 - (d) Quantity;
 - (e) Experimental protocol; and
 - (f) Availability of preventive measures and treatments.

Appendix C: Risk Groups - Selected Examples

Agents not listed in Risk Groups (RG) 2, 3, and 4 in what follows are not implicitly classified in RG 1.

(1) Risk Group 1 (RG1) agents are not associated with disease in healthy adult humans.

(a) Bacterial agents: *Bacillus subtilis* and *Escherichia coli* K-12

(2) Risk Group 2 (RG2) agents are associated with human diseases that are rarely serious, and often have preventive or therapeutic interventions available.

(a) Bacterial agents: *Bacillus anthracis*, *Escherichia coli* O157:H7, *Legionella* species, *Staphylococcus aureus*, *Streptococcus pneumoniae*, and *Vibrio cholera*.

(b) Fungal agents: *Blastomyces dermatitidis* and *Cryptococcus neoformans*.

(c) Parasitic agents: *Entamoeba histolytica* and *Giardia* species.

(d) Viral agents: Hepatitis viruses, Cytomegalovirus, Epstein Barr virus, and Parvoviruses.

(3) Risk Group 3 (RG3) agents are associated with serious or lethal human disease for which preventive or therapeutic interventions may be available (high individual risk but low community risk).

(a) Bacterial agents: *Brucella* sp., *Coxiella burnetii*, and *Mycobacterium tuberculosis*.

(b) Fungal agents: *Coccidioides immitis* and *Histoplasma capsulatum*.

(c) Viral agents: Hantaviruses and human immunodeficiency viruses.

(4) Risk Group 4 (RG4) agents are likely to cause serious or lethal human disease for which preventive or therapeutic interventions are not usually available (high individual risk and high community risk).

(a) Viral agents: Ebola virus and Monkey B virus.

Appendix D: Biosafety Level Classifications

- (1) Biosafety Level 1 (BSL-1) laboratories are suitable for work involving fixed/inactivated biological materials and well-characterized agents not known consistently to cause disease in healthy adults and that present minimal potential hazard to laboratory personnel and the environment. Work is typically conducted on open bench tops using standard microbiological practices. Special containment equipment or facility design is not required, but may be used as determined by an appropriate risk assessment. Some examples of BSL-1 activities include handling of inactivated human specimens and working with RG 1 agents.
- (2) Biosafety Level 2 (BSL-2) laboratories are suitable for work involving agents that pose moderate hazards to personnel and the environment. With good microbiological techniques and the appropriate safety equipment and facility designs, these agents can be used safely in activities conducted on the open bench, provided the potential for producing splashes and aerosols is low. These agents are typically transmitted by cuts, ingestion, or mucous membrane exposure. Some examples of BSL 2 activities include handling of human blood and blood products, handling of human and non-human primate cell lines and/or tissues, and working with Risk Group 2 agents.
- (3) Biosafety Level 3 (BSL-3) laboratories are suitable for work involving agents with a potential for respiratory transmission, and which may cause serious and potentially lethal infection. Microorganisms such as *Mycobacterium tuberculosis* and *Coxiella burnettii* are manipulated at BSL-3.
- (4) Biosafety Level 4 (BSL-4) laboratories are suitable for work involving dangerous agents that post a high individual risk of life-threatening disease, which may be transmitted via the aerosol route and for which there is no available vaccine or therapy. Viruses such as Marburg or Congo-Crimean hemorrhagic fever are manipulated at BSL-4.

Appendix E: Recommended Practices for Working in Biological Safety Cabinets

- (1) If the cabinet has been shut down, the blower should be operated for at least 10 minutes to allow the cabinet to purge before work begins again.
- (2) The work surface, the interior walls, and the interior surface of the window sash should be wiped with 70% ethanol or a freshly prepared 10% bleach solution before and after work. When bleach is used, a second wiping with 70% ethanol or sterile water is needed to remove the residual chlorine to prevent corrosion.
- (3) The front and rear perforated grills should be clutter free.
- (4) Overcrowding inside the BSC should be avoided.
- (5) Sudden movements in and out of and sweeping across the front grille of the BSC should be avoided.
- (6) Flame sources should not be used in the BSC.
- (7) All work materials including aerosol-generating equipment should be placed as far back in the cabinet as practical.
- (8) Biohazard waste bags should not be taped to the side of the cabinet.
- (9) Upright pipet collection containers should not be used in a BSC nor placed on the floor outside the cabinet. Only horizontal pipet discard trays containing an appropriate chemical disinfectant or disposable pipet container should be used inside the cabinet.

Appendix F: Recommended Procedures for Cleaning Up Spills of Biohazardous Materials

(1) Spills inside the BSC

Allow the BSC to run during clean-up. Cover spill with disinfectant-soaked paper towel or other absorbent materials. Carefully pour additional disinfectant solution around the edges of the spill and then into the spill. Avoid splashing. Allow a 20 minute contact period. Use paper towels or other absorbent materials to wipe up the spill, working from the outer edges into the center. Discard clean-up materials and gloves into biohazardous waste bin for autoclaving.

(2) Spills in the laboratory, outside the BSC.

Alert personnel in the immediate area of spill. Remove any contaminated clothing and place in biohazardous waste bin. Keep the BSC running or turn it on. Leave the area for approximately 30 minutes for the aerosols to settle before re-entering. Re-enter with disposable gown, shoe covers, face shield or eye protection and N-95 mask, and gloves. Cover spill with disinfectant-soaked paper towel or other absorbent materials. Carefully pour additional disinfectant solution around the edges of the spill and then into the spill. Avoid splashing. Allow a 20 minute contact period. Use paper towels or other absorbent materials to wipe up the spill, working from the outer edges into the center. Discard clean-up materials, disposable gown, gloves, and shoe covers into biohazardous waste bin for autoclaving.

(3) Spill in a centrifuge without safety buckets

A spill inside a centrifuge has the potential for multiple infections from a single incident. Aerosols are generated when fluid escapes from the rotor or cup while the centrifuge is operating at high speed. All opening of centrifuges must be performed slowly. If a centrifuge tube breaks while the centrifuge is running, turn off the motor. Allow the machine to be at rest for 30 minutes before opening. If breakage/leakage is observed after the centrifuge has stopped, re-close the lid immediately and allow the machine to be at rest for 30 minutes. Unplug centrifuge before initiating clean-up. Don puncture resistant gloves, lab coat, face shield or eye protection and N-95 mask before proceeding with clean-up. Flood the centrifuge bowl with disinfectant. Remove buckets and rotors to BSC for thorough chemical disinfection with a minimum contact time of 20 minutes. Discard clean-up materials and gloves into biohazardous waste bin for autoclaving. The use of sealable safety buckets in centrifuge is strongly recommended.

(4) Spill in a centrifuge with safety buckets

Transfer the sealed bucket to a BSC before opening. Remove leaked tube and dispose into biohazardous waste bin inside the BSC. Soak bucket with disinfectant for a minimum contact time of 20 minutes. Discard clean-up materials and gloves into biohazardous waste bin for autoclaving.

(5) Spill outside the laboratory during transport on campus

Alert personnel in the immediate public area of the spill. Do not attempt to clean-up the spill without appropriate PPE. Return with disinfectant, absorbent materials, and a disposable biohazardous waste bag. Don lab coat, shoe covers, face shield or eye protection and N-95 mask, and gloves. Cover spill with disinfectant-soaked absorbent materials. Carefully pour additional disinfectant solution around the edges of the spill and then into the spill. Avoid splashing. Allow a 20 minute contact period. Use absorbent materials to wipe up the spill, working from the outer edges into the center. Discard clean-up materials, gloves, and shoe-covers into the disposable biohazardous waste bag. Return the disposable biohazardous waste bag into the lab for proper disposal.

Appendix G: Recommended Procedures for Autoclaving Biohazardous Materials

- (1) The autoclavable biohazardous waste bag should be autoclaved when three-quarters full.
- (2) Bags should be handled while wearing gloves and lab coat.
- (3) When removing the bags from the waste collection bins, the bags should be immediately knotted or tied off.
- (4) The temperature of the autoclave must be at least 121°C (250°F) with a minimum pressure of 15 psi. The waste must be treated for a minimum of 45 minutes in a liquid cycle.
- (5) A sterilization indicator strip should be run with each cycle.
- (6) Routine autoclave efficacy monitoring using a biological indicator such as *Bacillus stearothermophilus* ampoule should be conducted at least monthly.
- (7) Once the waste has been treated, it can be placed in a regular household garbage bag, tied up, and picked up by custodians.
- (8) Date of treatment, name of person who performs the treatment, method/conditions of treatment, and verification of operating parameters or biological monitoring should be properly documented.

Appendix H: Emergency Response Procedures – Examples

(1) Biohazardous spills on body

- (a) Flood exposed skin with running water from faucet or safety shower for at least 15 minutes.
- (b) Remove all contaminated clothing and shoes and dispose of them in a biohazard waste receptacle.
- (c) Seek medical attention if needed.
- (d) Report the incident to a supervisor as soon as possible and file a work-related injury report via **IRIS**.

(2) Biohazardous materials splashed in the eye

- (a) Immediately rinse eyeball and inner surface of eyelid continuously with water for 15 minutes.
- (b) Hold the eyes open to effectively wash behind eyelids.
- (c) Seek medical attention if needed.
- (d) Report incident to supervisor as soon as possible and file a work-related injury report via **IRIS**.

(3) Needle sticks/cuts

- (a) Clean the puncture site with soap and flush it with water for at least 15 minutes.
- (b) Seek medical attention if needed.
- (c) Report incident to supervisor as soon as possible and file a work-related injury report via **IRIS**. Also fill out the OSHA Sharps Injury Log.

Bloodborne Pathogens

NIST S 7101.51

Document Approval Date: 03/18/2013

Effective Date: 04/01/2013

1. PURPOSE

The purpose of the Bloodborne Pathogens (BBP) suborder is to eliminate or minimize occupational exposure to bloodborne pathogens and other potentially infectious materials (OPIMs) in accordance with the Occupational Health and Safety Administration (OSHA) Standard for Bloodborne Pathogens, 29 CFR 1910.1030.

This suborder, together with the associated deployment tools, the schedule and method of implementation, the applicable OU job hazard classification and analysis procedures, and the associated hazard reviews for specific experiments, shall serve as the Bloodborne Pathogens Exposure Control Plan (ECP) for all NIST facilities.

2. BACKGROUND

None.

3. APPLICABILITY

- a. The provisions of this suborder apply to all NIST facilities and to all NIST employees who in carrying out their assigned duties could be exposed to bloodborne pathogens, with the following exceptions:

- (1) Those noted in [NIST O 710](#), Occupational Safety and Health; and

- (2) Workers at the NIST Child Care Center.

- b. NIST employees who work with biohazardous materials such as bacteria, fungi, viruses, parasites, rickettsia, biological toxins, recombinant DNA (deoxyribonucleic acid) materials, prions, and non-human mammalian blood, blood products, body fluids, cell lines, and tissues shall follow the requirements in the NIST Biosafety suborder.

39 **4. REFERENCES**

- 40 a. 29 CFR 1910.1030, Bloodborne Pathogens
41
42 b. Needle Stick Safety and Prevention Act, Amendment to 29 CFR 1910.1030
43
44

45 **5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS**

- 46 a. NIST 7101.50: Biosafety;
47
48 b. NIST 7101.20: Work and Worker Authorization Based on Hazard Reviews;
49
50 c. NIST 7101.22: Hazard Signage;
51
52 d. NIST 7101.24: Incident Reporting and Investigation; and
53
54 e. NIST 7101.21: Personal Protective Equipment.
55
56

57 **6. REQUIREMENTS**

- 58 a. Exposure Determinations
59

60 (1) Exposure determinations shall be conducted as part of the hazard review process to
61 identify employees' potential risk of occupational exposure to human blood or OPIMs as
62 defined by the OSHA Bloodborne Pathogens Standard. The exposure determination is
63 made without regard to the use of personal protective equipment (PPE).
64

65 (2) Employees identified as having a potential occupational exposure to human blood and
66 OPIMs must comply with the BBP Exposure Control Plan (ECP).
67

- 68 b. Compliance Methods

69 All of the following compliance methods shall be adhered to:
70

- 71 (1) Universal Precautions

72 According to OSHA, Universal Precautions are defined as the infection control practices
73 in which all human blood and OPIMs are treated as if known to be infectious for HBV,
74 HIV, and other bloodborne pathogens. The Universal Precaution approach is based on
75 the premise that a medical history and examination cannot reliably identify all people
76 infected with bloodborne pathogens. OSHA mandates that Universal Precautions shall be
77 observed to prevent contact with blood or other potentially infectious materials. Under

78 circumstances in which differentiation between body fluid types is difficult or impossible,
79 all body fluids shall be considered potentially infectious materials.
80

81 (2) Engineering Controls and Work Practice Controls

82 Engineering controls and work practice controls shall be used to eliminate or minimize
83 employee exposure. Where occupational exposure remains after instituting these
84 controls, personal protective equipment shall also be used. Engineering controls shall be
85 examined and maintained or replaced on a regular schedule to ensure their effectiveness.
86

87 i. Hand-washing

88
89 (i) Hand-washing facilities in the same room shall be readily accessible to
90 employees.
91

92 (ii) When provision of hand-washing facilities in the same room is not
93 feasible, the employer shall provide in the room an appropriate antiseptic
94 hand cleanser in conjunction with clean cloth/paper towels or antiseptic
95 towelettes. When antiseptic hand cleansers or towelettes are used, hands
96 shall be washed with soap and running water as soon as feasible.
97

98 (iii) Hands and skin surfaces must be washed immediately following contact
99 with human blood or OPIMs, at the conclusion of tasks that involve
100 blood and OPIMs, and after gloves are removed.
101

102 ii. Sharps control

103
104 (i) Contaminated needles and other sharps shall not be bent, recapped, or
105 removed. The exception to this is if it can be demonstrated that no
106 alternative is feasible or the action is required by a specific medical
107 procedure. If such action is required, then it must be accomplished
108 through the use of a mechanical device or a one-handed technique.
109 Shearing or breaking of contaminated needles is prohibited.
110

111 (ii) Contaminated sharps shall be discarded immediately, or as soon as
112 feasible, in containers that are closable, puncture resistant, leak-proof on
113 sides and bottom, and biohazard labeled or color-coded.
114

115 (iii) Containers for contaminated sharps shall be kept in the same room and
116 be easily accessible to personnel and replaced before they become three-
117 quarters full. Once sharps containers containing contaminated waste

have been closed, they should be placed in a medical waste box for disposal. In Gaithersburg and Boulder, OSHE will pick-up and dispose of medical waste boxes upon request.

- (iv) When moved from the area of use, containers of sharps shall be closed immediately prior to removal to prevent spillage or protrusion of contents during handling, storage, transport, or shipping.
- (v) Primary containers of contaminated sharps shall be placed in a secondary container if leakage of the primary container is possible. The secondary container shall be closable; constructed to contain all contents and prevent leakage during handling, storage, transport, or shipping; and labeled or color-coded.
- (vi) When the elimination of needle-bearing devices is not possible, needle devices with safety features should be utilized.
- (vii) Reusable sharps and reusable sharps containers are not permitted at NIST.

iii. Containment Equipment

- (i) Engineering controls such as biosafety cabinets, fume hoods, sealed centrifuge rotors, sealed centrifuge safety cups, or bench top splash shields shall be used for blood and OPIMs procedures that could potentially generate splashes and droplets. Such procedures include centrifuging, grinding, vortexing, blending, transferring liquids, homogenizing, withdrawing liquids under pressure, and opening containers of infectious materials having internal pressures different from ambient pressure.

iv. Standard Safe Work Practices

- (i) Eating, drinking, smoking, applying cosmetics or lip balm, and handling contact lenses are prohibited in work area.
- (ii) Food and drink shall not be kept in refrigerators, freezers, shelves, cabinets, or on countertops or bench tops where blood or OPIMs are present.

- 158 (iii) All procedures involving blood or OPIMs shall be performed in a
159 manner that minimizes splashing, spraying, splattering, and generating
160 droplets of these substances.
- 161
- 162 (iv) Mouth pipetting/suctioning of blood or OPIMs is prohibited. Use
163 mechanical pipetting devices.
- 164
- 165 (v) Equipment that may become contaminated with blood or OPIMs shall be
166 examined prior to servicing or shipping and shall be decontaminated as
167 necessary unless the decontamination of the equipment is not feasible.
168 A readily observable biohazard label shall be attached to the equipment
169 stating which portions remain contaminated. The information must be
170 conveyed to all affected employees, the servicing representative, and/or
171 the manufacturer, prior to handling, servicing, or shipping so that the
172 appropriate precautions will be taken.
- 173
- 174 (vi) If eyes are exposed to potentially infectious materials, they should be
175 immediately flushed with water for at least 15 minutes, after which a
176 medical evaluation must be obtained. A medical evaluation must be
177 obtained immediately when other percutaneous or mucous membrane
178 exposures occur.
- 179
- 180 (vii) Specimens of blood or OPIMs shall be placed in containers that prevent
181 leakage during collection, handling, processing, storage, transport, or
182 shipping. The container for storage, transport, or shipping shall be
183 biohazard labeled.
- 184
- 185 (viii) If outside contamination of a primary container occurs, the primary
186 container shall be placed within a second container that prevents leakage
187 during the handling, processing, storage, transport, or shipping. The
188 outside of the secondary container shall be biohazard labeled.
- 189
- 190 (ix) If the specimens could puncture the primary container, the primary
191 container shall be placed within a puncture-resistant secondary
192 container.
- 193

194 (3) Personal Protective Equipment

195

- 196 (a) Appropriate PPE shall be provided at no cost to employees. Appropriate PPE
197 includes, but is not limited to gloves, gowns, laboratory coats, face shields or masks

and eye protection, shoe-covers, mouthpieces, resuscitation bags, pocket masks, or other ventilation devices.

(b) PPE must be chosen according to the NIST Personal Protective Equipment Suborder, and each OU's Hazard Review procedure.

(c) PPE is chosen based on the anticipated exposure to blood or OPIMs. PPE is considered appropriate only if it does not permit blood or OPIMs to pass through or reach the employee's clothing, skin, eyes, mouth, or other mucous membranes under normal conditions of use and for the duration of the time the protective equipment is used.

(d) Appropriate protective clothing such as, but not limited to, gowns, aprons, lab coats, clinic jackets, or similar outer garments shall be worn in occupational exposure situations. The type and characteristics will depend upon the task and degree of exposure anticipated.

(e) Appropriate PPE in the appropriate sizes must be readily accessible.

(f) All PPE shall be cleaned, laundered, or disposed of at no cost to the employee. Contaminated PPE shall never be taken home for laundering.

(g) PPE shall be repaired or replaced as needed to maintain its effectiveness at no cost to employees.

(h) The following PPE practices shall be adhered to:

- i. If a garment(s) is penetrated by blood or OPIMs, the garment(s) shall be removed immediately or as soon as feasible.
- ii. All PPE shall be removed prior to leaving the work area.
- iii. When PPE is removed, it shall be placed in an appropriately designated area or container for storage, washing, decontamination, or disposal.
- iv. Gloves shall be worn when it can be reasonably anticipated that the employee may have hand contact with blood, OPIMs, mucous membrane, and non-intact skin; when performing vascular access procedures; and when handling or touching contaminated items or surfaces.

- v. Hypoallergenic gloves, glove liners, powderless gloves, or other similar alternatives shall be readily accessible to those employees who are allergic to the gloves normally provided.
- vi. Disposable gloves shall be replaced as soon as feasible when contaminated, torn, or punctured. Disposable gloves shall not be washed or decontaminated for re-use.
- vii. Utility gloves may be decontaminated for re-use if the integrity of the glove is not compromised. However, they must be discarded if they are cracked, peeling, torn, or punctured.
- viii. Masks in combination with eye protection devices, such as goggles or glasses with solid side shields, or stand-alone chin-length face shields shall be worn whenever splashes spray, splatter, or droplets of blood or OPIMs may be generated and eye, nose, or mouth contamination can be reasonably anticipated.

(4) Housekeeping

- (a) The worksite shall be maintained in a clean and sanitary condition by adhering to the following:

- i. All work surfaces and equipment are to be decontaminated after completion of procedures, immediately or as soon as feasible when surfaces have been overtly contaminated or after any spill of blood or OPIMs, and at the end of the work shift if the surface has been contaminated since the last cleaning.
- ii. Protective coverings, such as plastic wrap, aluminum foil, or imperviously-backed absorbent paper used to cover equipment and environmental surfaces are to be removed and replaced as soon as feasible when they become overtly contaminated or at the end of the work shift if they may have become contaminated during the shift.
- iii. All bins, pails, cans, and similar receptacles intended for reuse which have a reasonable likelihood for becoming contaminated with blood or other potentially infectious materials shall be inspected and decontaminated on a regularly scheduled basis and cleaned and decontaminated immediately or as soon as feasible upon visible contamination.

- 278 iv. Any broken glassware which may be contaminated is not to be picked up
279 directly with the hands. It shall be cleaned up using mechanical means, such
280 as a brush and dust pan, tongs, or forceps.
- 281
- 282 v. Appropriate disinfectants shall be used for routine decontamination of work surfaces and
283 equipment and spill clean-ups. Freshly prepared 10% bleach solution is the disinfectant
284 of choice for blood and OPIMs. Other EPA approved tuberculocidal disinfectants are the
285 only acceptable disinfectants; a list of such disinfectants can be accessed at
286 http://www.epa.gov/oppad001/list_b_tuberculocide.pdf . Disinfectants must be in
287 contact with work surfaces, equipment (where appropriate, refer to equipment manual for
288 decontamination instruction), or spills for at least 20 minutes before cleaning. Cleanups
289 in the laboratories shall be conducted by Laboratory staff members that have been trained
290 on biological spill cleanups. Contact OSHE for assistance if needed.
- 291
- 292 vi. For Boulder personnel, pools of blood or body fluids resulting from injuries
293 shall be cleaned up by the Boulder Safety Office.
- 294

295 (5) Regulated Waste Disposal

296

- 297 (a) All contaminated sharps shall be discarded as described in 8.b(2)(b).
- 298
- 299 (b) All other regulated waste such as pipettes, centrifuge tubes, cell cultures, and human
300 specimens should be placed in labeled or color-coded biohazard waste containers that
301 are closable and constructed to contain all contents and to prevent leakage of fluids
302 during handling, storage, transport, or shipping.
- 303
- 304 (c) Biohazard waste receptacles shall remain upright during use and be disposed of
305 routinely when three-quarters full.
- 306
- 307 (d) If outside contamination of the waste container occurs, it shall be placed in a labeled
308 or color-coded second container that is closable and constructed to contain all
309 contents and to prevent leakage of fluids during handling, storage, transport or
310 shipping.
- 311
- 312 (e) In Gaithersburg and Boulder, OSHE will pick-up and dispose of medical waste boxes
313 upon request. Waste generators are expected to submit pickup requests, limit the
314 loading of each medical waste box to less than 40 pounds, store sealed medical waste
315 boxes in the work area in which they were generated or in the adjacent service galley,
316 not in common hallways.
- 317

318 (6) Laundry

- 319
- 320 (a) Any garment penetrated by blood or OPIMs shall be removed immediately, or as
- 321 soon as feasible and handled as little as possible, using gloves and any other
- 322 appropriate universal precautions. Contaminated laundry shall be bagged or
- 323 containerized at the location where it was used and placed in an appropriately labeled
- 324 (biohazard symbol) container or leak proof bag prior to laundering.
- 325
- 326 (b) Soiled laundry shall be processed by an outside contractor that specifically cleans lab
- 327 coats or contaminated laundry. Soiled laundry must be placed in a labeled laundry
- 328 bag for transport.
- 329
- 330 (c) For NIST facilities that do not have contracted laundry services, disposable gowns
- 331 shall be used. Worn disposable gowns shall be replaced monthly at a minimum or
- 332 when contaminated. Contaminated gowns shall be discarded in biohazard waste
- 333 receptacles.
- 334

335 For specific tasks and employee work practices, refer to Appendix B.

336

337 c. Hepatitis B Vaccination

338

- 339 (1) All employees except for Facility Users who have been identified as having potential
- 340 occupational exposure to blood or OPIMs shall be offered the hepatitis B vaccine by their
- 341 OUs at no cost. The vaccine is offered after bloodborne pathogen training and within 10
- 342 working days of their initial assignment to work unless the employee has previously
- 343 received the complete hepatitis B vaccination series, antibody testing has revealed that
- 344 the employee is immune, or the vaccine is contraindicated for medical reasons.
- 345 Participation in a prescreening program shall not be a prerequisite for receiving hepatitis
- 346 B vaccination. The vaccine shall be administered by the workplace health unit or, if the
- 347 workplace does not have a health unit that administers vaccine, a licensed healthcare
- 348 professional. If an employee chooses to decline vaccination, the employee must sign a
- 349 declination form. Employees who decline may request and obtain the vaccination at a
- 350 later date at no cost. Refer to Appendix C for a Hepatitis B vaccine declination form.
- 351
- 352 (2) For NIST workplaces that do not offer Hepatitis B vaccines onsite, employees may obtain
- 353 the vaccination during normal work hours from any licensed healthcare facility or
- 354 professional. The vaccination cost and travel cost shall be reimbursed by the division
- 355 according to the OU's reimbursement procedures.
- 356

(3) If a routine booster dose of the vaccine is recommended by the U.S. Public Health Service (PHS) at a future date, the booster doses are to be made available at no cost to the employees. OSHA shall review the U.S. PHS's recommendations for vaccine boosters during the annual review of this suborder.

(4) All Hepatitis B vaccine records or declination forms shall be kept by the workplace health unit, or if the workplace does not have a health unit that maintains these records, by the employee's division administrative office.

d. Post-Exposure Evaluation and Follow-Up

(1) Employees shall immediately notify their supervisor of an exposure incident and an incident report must be completed and submitted through NIST's Incident Reporting and Investigation System (IRIS) in accordance with the requirements of the NIST Incident Reporting and Investigation Suborder.

(2) Following an exposure incident report, a no cost confidential medical evaluation and follow-up during normal work hours that includes at least the following elements shall be made available immediately to the exposed employee:

(a) Documentation of the route(s) of exposure and the circumstances under which the exposure incident occurred;

(b) Identification and documentation of the source individual, unless the employer can establish that identification is infeasible or prohibited by state or local law;

(c) Testing of the source individual's blood as soon as feasible and after consent is obtained in order to determine HBV and HIV infectivity;

i. Results of the source individual's testing shall be made available to the exposed employee. When the source individual is already known to be infected with HBV or HIV, testing for the source individual's known HBV or HIV status need not be repeated.

(d) Collection of the exposed employee's blood as soon as feasible and testing after consent is obtained; and

i. The blood sample shall be preserved for up to 90 days to allow the employee to decide if their blood should be tested for HBV and HIV serological status.

- 397 (e) Post-exposure prophylaxis, counseling, and evaluation of reported illnesses.
398
- 399 (3) If the exposure results from a contaminated sharps injury, the incident shall be recorded
400 on the sharps injury log (see Appendix F).
401
- 402 (4) The evaluating healthcare professional will be provided with the following information:
403
- 404 (a) A copy of the OSHA Bloodborne Pathogen regulations (29 CFR 1910.1030);
405
- 406 (b) A description of the route of exposure and circumstances under which exposure
407 occurred;
408
- 409 (c) A description of the employee's duties as they relate to the exposure incident;
410
- 411 (d) Results of the source individual's blood testing, if available; and
412
- 413 (e) Any medical records which are relevant to the appropriate treatment of the employee,
414 including vaccination status, and which are the employer's responsibility to maintain.
415
- 416 (5) A copy of the evaluating healthcare professional's written opinion shall be obtained by
417 the OU and provided to the exposed employee within 15 days after evaluation. The
418 healthcare professional's written opinion for Hepatitis B vaccination shall be limited to
419 whether Hepatitis B vaccination is indicated for an employee, and if the employee has
420 received such vaccination. The opinion shall state that the employee has been informed
421 of the results of the evaluation and that the employee has been told about any medical
422 conditions resulting from exposure to blood or OPIMs that require further evaluation or
423 treatment. Refer to Appendix D for the Healthcare Professional's Opinion Form for
424 Bloodborne Pathogens Post-Exposure Evaluation and Follow-up.
425
- 426 (6) All other unrelated findings or diagnoses shall remain confidential and shall not be in the
427 written report.
428
429
430
431
432
433
434
435
436

e. Communication of Hazards to Employees

(1) Labels and Signs

(a) Labels

- i. Biohazard warning labels shall be affixed to containers of regulated waste; refrigerators and freezers containing blood or OPIMs; and other containers used to store, transport, or ship blood or other OPIMs.
- ii. Labels shall include the biohazard symbol and the word “Biohazard.” These labels shall be fluorescent orange or orange-red, or predominantly so, with lettering and biohazard symbol in a contrasting color as in Figure 1. Red bags or red containers may be substituted for labels.



Figure 1. Biohazard label

- iii. Labels shall either be an integral part of the container or shall be affixed as close as possible to the container by string, wire, adhesive, or other method that prevents their loss or unintentional removal.
- iv. Individual containers of blood or OPIMs that are placed in a labeled container during storage, transport, shipment or disposal are exempted from the labeling requirement.
- v. Regulated waste that has been decontaminated need not be labeled or color coded.

(b) Signs

- i. Biohazard signs shall be posted at the entrance to work areas where blood and OPIMs are handled. The signs shall be in compliance with the NIST Hazard Signage Suborder. See Figure 2 below. Employees can request biohazard signs in accordance to the NIST Hazard Signage Suborder.



Figure 2. Biohazard signage

(2) Training

- (a) Training shall be provided in accordance with the requirements of the NIST Safety Education and Training Suborder.
- (b) Bloodborne-pathogens training shall include the content described in Appendix E.
- (c) Initial bloodborne-pathogens training provided by an OSHE instructor shall be completed by new employees, including newly reassigned employees, prior to their working with materials that could result in their exposure to bloodborne pathogens or OPIMs. Current employees who have completed the bloodborne-pathogens training module in the Commerce Learning Center are exempt from having to meet this requirement.
 - i. Completion of State- or County-provided bloodborne-pathogens training will meet this requirement.
- (d) Refresher bloodborne-pathogens training specified by OSHE online shall be completed online by employees annually.

f. Documentation/Recordkeeping

(1) Training Records:

(a) All initial and refresher bloodborne-pathogen training shall be documented, recorded, and maintained for at least three years by OSHA in accordance with the requirements of the NIST Safety Education and Training Suborder. Documentation and records shall include the following:

- i. The dates of the training sessions;
- ii. The contents or a summary of the training sessions;
- iii. The names and qualifications of persons conducting the training; and
- iv. The names and job titles of all persons attending the training sessions.

(b) Employee training records shall be provided upon request for examination and copying to employees, and to employee representatives.

(2) Medical Records

(a) Accurate records for each employee with an occupational exposure shall be established and maintained in accordance with 29 CFR 1910.20 by the workplace health unit, or if the workplace does not have a health unit that establishes and maintains such records, by the covered employee's division administrative office. This record shall include:

- i. The name and social security number of the employee;
- ii. A copy of the employee's hepatitis B vaccination status including the dates of all the hepatitis B vaccinations and any medical records relative to the employee's ability to receive vaccination;
- iii. A copy of all results of examinations, medical testing, and follow-up procedures;
- iv. A copy of the healthcare professional's written opinion; and
- v. A copy of the information provided to the healthcare professional.

(b) The medical records shall be kept confidential and maintained for at least the duration of employment plus 30 years with the exceptions of health insurance claims records; first aid records of one-time treatment and subsequent observation of minor scratches, cuts, burns, splinters, and the like which do not involve medical treatment; and medical records of employees who have worked for less than one year if the records are provided to the employee upon termination.

(c) The medical records shall not be disclosed or reported to any person within or outside the workplace without the covered employee's express written consent except as required by this section or as may be required by law.

(d) Employee medical records shall be provided upon request for examination and copying to employees and to employee representatives.

(3) Transfer of Training and Medical Records

(a) The requirements involving transfer of records set forth in 29 CFR 1910.1020(h) shall be met by the transferring party.

(4) Sharps Injury Log

(a) A sharps injury log shall be maintained by the division for the recording of percutaneous injuries from contaminated sharps. Refer to Appendix F for an example of a Sharps Injury Log. Alternative Sharps Injury Logs are acceptable.

(b) The information in the sharps injury log shall be recorded and maintained in a manner that protects the confidentiality of the injured employee.

(c) The log shall be completed by division personnel and maintained by the division for at least six years.

(d) The sharps injury log shall contain, at a minimum:

i. Type and brand of device involved in the incident;

ii. Work area where the exposure incident occurred; and

iii. Explanation of how the incident occurred.

- (e) The Sharps Injury Log shall be reviewed at least once a year by division personnel.
Sharps and procedures that are frequently documented in the log shall be replaced by
safer alternatives.

7. DEFINITIONS

- a. Blood - Human blood, human blood components, and products made from human blood.
- b. Bloodborne Pathogens - Pathogenic microorganisms that are present in human blood, and can cause disease in humans. These pathogens include, but are not limited to, Human Immunodeficiency Virus (HIV), Hepatitis B Virus (HBV), and Hepatitis C Virus (HCV). Refer to Appendix A for detailed descriptions.
- c. Clinical Laboratory – A workplace where diagnostic or other screening procedures are performed on blood or OPIMs.
- d. Contaminated – The presence or the reasonably anticipated presence of blood or OPIMs on an item or surface.
- e. Contaminated Laundry – Laundry soiled with blood or OPIMs, or that may contain sharps.
- f. Contaminated Sharps – Any contaminated object that can penetrate the skin, including, but not limited to, needles, scalpels, lancets, broken glass, broken capillary tubes, and exposed ends of dental wires.
- g. Continuous/established human cell lines – Immortalized cells that have been transformed by spontaneous mutation or natural or laboratory infection with an immortalization agent, and then propagated or passed many times.
- h. Decontamination – The use of physical or chemical means to remove, inactivate, or destroy bloodborne pathogens on a surface or item to the point where they are no longer capable of transmitting infectious particles and the surface or item is rendered safe for handling, use, or disposal.
- i. Engineering Controls – Controls (e.g., sharps disposal containers, self-sheathing needles, safer medical devices, such as sharps with engineered sharps injury protections, and needleless systems) that isolate or remove the bloodborne pathogens hazard from the workplace.

- j. Exposure Incident – A specific eye, mouth, other mucous membrane, non-intact skin, or parenteral contact with blood or OPIMs that result from the performance of a covered employee’s duties.
- k. Facility User – Any individual who is permitted to use designated NIST facilities under a NIST Facility Use Agreement. Designated NIST facilities include the NIST Center for Neutron Research and the Center for Nanoscale Science and Technology.
- l. Hand Washing Facilities – A facility providing an adequate supply of running potable water, soap, and single use towels or air drying machines.
- m. Hepatitis B Virus (HBV) – A virus that may be contracted through exposure to blood and/or body fluids and can result in acute and chronic liver diseases.
- n. Hepatitis C Virus (HCV) – A virus that may be contracted through exposure to blood and/or body fluids and can result in chronic liver diseases.
- o. Human Immunodeficiency Virus (HIV) – A virus that may be contracted through blood and/or body fluids and can result in Acquired Immune Deficiency Syndrome (AIDS), a condition in which the body is unable to fight infections.
- p. Licensed Healthcare Professional – A person whose legally permitted scope of practice allows him or her to independently evaluate an individual and determine appropriate interventions, such as hepatitis B vaccination and post-exposure evaluation and follow-up.
- q. Medical or Infectious Waste – Infectious human or animal waste generated or produced as a result of research, a medical diagnosis, treatment, or immunization.
- r. Needleless System – A medical device that does not use needles for:
- (1) The collection of bodily fluids or withdrawal of body fluids after initial venous or arterial access is established;
 - (2) The administration of medication or fluids; or
 - (3) Any other procedure with potential percutaneous exposure to a contaminated sharp.
- s. Occupational Exposure – Reasonably anticipated skin, eye, mucous membrane, or parenteral contact with blood or other potentially infectious materials that may result from the performance of a covered employee’s duties.

- t. Other Potentially Infectious Materials (OPIMs) include:
- (1) The following human body fluids: semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, pericardial fluid, peritoneal fluid, amniotic fluid, saliva in dental procedures, any body fluid that is visibly contaminated with blood, and all body fluids in situations where it is difficult or impossible to differentiate between body fluids;
 - (2) Any unfixed tissue or organ (other than intact skin) from a human (living or dead);
 - (3) HIV, HBV, or HCV containing human cells or tissue cultures, organ cultures, and culture media or other solutions;
 - (4) Primary and continuous/established human cell lines; and
 - (5) Blood, organs, or other tissues from experimental animals infected with HIV or HBV.
- u. Parenteral – Piercing mucous membranes or the skin barrier through such events as needle sticks, human bites, cuts, and abrasions.
- v. Personal Protective Equipment (PPE) – Specialized clothing or equipment worn by an employee for protection against a hazard. General work clothes (e.g., uniforms, pants, shirts or blouses) not intended to function as protection against a hazard are not considered to be personal protective equipment.
- w. Primary human cell lines – Propagated in vitro from primary explants of human tissue or body fluids that have a finite lifetime in tissue culture for 20 passages to 70 passages.
- x. Regulated Medical Waste – Liquid or semi-liquid blood or other potentially infectious materials; contaminated items that would release blood or other potentially infectious materials in a liquid or semi-liquid state if compressed; items that are caked with dried blood or other potentially infectious materials and are capable of releasing these materials during handling; contaminated sharps; and pathological and microbiological wastes containing blood or other potentially infectious materials.
- y. Sharps – Any object that can reasonably be anticipated to penetrate the skin or any other body part, which includes, but is not limited to, needle devices; scalpels; lancets; a piece of broken glass; a broken capillary tube; an exposed end of a wire; or a knife, drill, or bur.
- z. Sharps with Engineered Sharps Injury Protection – A non-needle sharp or sharp device used for withdrawing body fluids, accessing a vein or artery, or administering medications or other

708 fluids, with built-in safety features or mechanisms that effectively reduce the risk of an
709 exposure incident.

710
711 aa. Source Individual – Any individual, living or dead, whose blood or OPIMs may be a source
712 of occupational exposure to covered employees.

713
714 bb. Sterilize – The use of a physical or chemical procedure to destroy all microbial life, including
715 highly resistant bacterial endospores.

716
717 cc. Universal Precautions – An approach to infection control, wherein all human blood and
718 OPIMs are treated as if known to be infectious for HIV, HBV, HCV, and other bloodborne
719 pathogens.

720
721 dd. Work Practice Controls – Controls that reduce the likelihood of exposure by altering the
722 manner in which a task is performed (e.g., prohibiting recapping of needles by a two-handed
723 technique).

724
725
726 **8. ACRONYMS**

727 a. BBP – Bloodborne Pathogens

728
729 b. BSC – Biological Safety Cabinet

730
731 c. CDC – Centers for Disease Control and Prevention

732
733 d. CFR – Code of Federal Regulations

734
735 e. CLC – Commerce Learning Center

736
737 f. CPR – Cardiopulmonary Resuscitation

738
739 g. ECP – Exposure Control Plan

740
741 h. HBV – Hepatitis B Virus

742
743 i. HCV – Hepatitis C Virus

744
745 j. HIV – Human Immunodeficiency Virus

746
747 k. NIH – National Institutes of Health

748 l. NIST – National Institute of Standards and Technology

749 m. OPIMs – Other Potentially Infectious Materials

750 n. OSHA – Occupational Safety and Health Administration

751 o. PPE – Personal Protective Equipment

756 9. RESPONSIBILITIES

757 a. Employees are responsible for:

758 (1) Ensuring the safety of sponsored visitors unfamiliar with the requirements of the
759 Bloodborne Pathogens suborder.

760 b. OSHE Bloodborne Pathogens Program Manager is responsible for:

761 (1) Providing OUs a list of all job classifications in which all employees in those job
762 classifications have occupational exposure; a list of job classifications in which some
763 employees have occupational exposure; and a list of all tasks and procedures or groups of
764 closely related task and procedures in which occupational exposure occurs and that are
765 performed by employees in job classifications listed.

771 10. AUTHORITIES

772 There are no authorities specific to this suborder alone.

775 11. DIRECTIVE OWNER

776 Chief Safety Officer

779 12. APPENDICES

780 a. Appendix A. Overview of Major Bloodborne Pathogens

781 b. Appendix B. Work Practices for Specific Employees or Tasks

782 c. Appendix C. Hepatitis B Vaccine Declination Form

- 787 d. Appendix D. Healthcare Professional's Written Opinion Form for Bloodborne Pathogens
- 788 Post Exposure Evaluation and Follow-up
- 789
- 790 e. Appendix E. Bloodborne Pathogens Training Contents
- 791
- 792 f. Appendix F. Sharps Injury Log

Appendix A: Overview of Major Bloodborne Pathogens

(1) Hepatitis B Virus (HBV)

The Hepatitis B virus can cause inflammation of the liver, lifelong infection, cirrhosis (scarring) of the liver, liver cancer, liver failure, and death. The incubation period can be as long as 160 days, with an average of 120 days. Symptoms and signs include anorexia, malaise, nausea, vomiting, abdominal pain, and jaundice. Carriers are capable of passing the disease to others through blood and body fluids. HBV is commonly transmitted through the use of contaminated needles. Workers exposed to infected blood are the most at risk. Vaccines are available.

(2) Hepatitis C Virus (HCV)

Like HBV, HCV also causes inflammation of the liver and chronic liver disease. HCV is primarily spread through contact with infected blood. The potential for HCV transmission associated with percutaneous injury is low, varying between 3 and 10%. Although the HCV can be detected in blood between one to three weeks after the initial exposure, 80 percent of people with hepatitis C have no symptoms, and thus go undiagnosed. Most patients begin to develop liver cell injury within approximately 50 days, although they will be asymptomatic (symptom-free for the first 6 to 7 weeks after exposure). In about 15 percent of people exposed to the virus, their bodies naturally clear it out of their system within six months. The remaining 85 percent of people with hepatitis C will develop some level of chronic hepatitis C. Over time, this can cause serious liver damage, although the rate of progression can vary significantly from individual to individual. Symptoms may include fatigue, loss of appetite, jaundice, dark colored urine, abdominal pains, aches and pains, joint pain, nausea, and vomiting. Serious complications include liver failure caused by chronic infection. Treatment includes interferon and oral ribavirin, or a combination of the two medications. No vaccines are currently available for HCV.

(3) Human Immunodeficiency Virus (HIV)

HIV is transmitted through sexual contact or exposure to infected blood. Although the virus has been found in many body fluids, it is most commonly transmitted by contact with contaminated blood, semen, and vaginal secretions. Symptoms of infection include lack of energy, fatigue, weight loss, frequent fevers, sweating, nausea, abdominal cramps, and vomiting. More severe symptoms occur with advanced states of infection. There is no vaccine currently available for HIV.

Appendix B: Work Practices for Specific Employees or Tasks

(1) Laboratory researchers

All laboratory researchers shall follow OSHA's universal precautions and use the appropriate PPE for all tasks that involve potential eye, mucous membrane, or skin contact with human blood or OPIMs. Face shields must be worn if splashing/splattering is anticipated.

(2) Infectious Waste Management Personnel

All personnel who package and handle infectious waste containers shall wear safety glasses and gloves during tasks where potential eye and skin contact with infectious materials may occur.

(3) Custodial Services

(a) This suborder does not apply to those custodial services personnel at NIST who are contractors. However, it is required that contractor custodial services personnel observe the signs and instructions posted on the laboratory/office entrance in order to minimize their exposure to human blood or OPIMs. If cleanup of human blood or OPIMs are to be performed by contractor custodial personnel, only those who have been trained on blood and OPIMs cleanups shall perform these duties.

(b) Routine cleanup and disinfection of bathrooms are not considered activities that fall under the requirements of 1910.1030. Custodial personnel who are responsible for housekeeping in bathrooms shall carefully handle razors that may be discarded in the common trash by wearing gloves and handling the razor with tongs or tweezers. If feminine hygiene products have been placed into the bathroom's common waste receptacle, and the receptacle is lined with a plastic bag, the bag may be removed and disposed as normal trash.

(4) Plumbing Activities

Most of the body fluids directed into the sanitary system are not regulated by 1910.1030. However, because several diseases are associated with exposure to sewage, all employees who are involved in plumbing activities shall be provided with the necessary equipment to prevent contact with sanitary effluent. Employees who clear sanitary drain blockages, including use of plungers and snaking, are not considered occupationally-exposed to human blood or OPIMs unless visible blood or other regulated body fluid is present in the work area. Appropriate PPE (e.g., gloves, eye protection, boots, etc.) shall be available to any worker clearing a blockage in sanitary drain systems or during sewage clean-up operations.

(5) Health Unit Personnel

All Health Unit personnel shall follow universal precautions during all tasks that involve potential eye, mucous membrane, or skin contact with human blood, bodily fluids, or OPIMs. Sharps precautions must also be followed.

(6) Police Services Group Personnel

All Police Services Group Personnel shall follow the infection control procedures developed and published at the Division/Group level.

(7) Fire Protection Group Personnel

All Fire Protection Group Personnel shall follow the infectious control procedures developed and published at the Division/Group level.

(8) NIST Vehicles

(a) Any blood or body fluids spilled in NIST vans and shuttle buses shall be cleaned up using an appropriate disinfectant and proper procedures. Minimum personal protective equipment shall include gloves and eye protection.

(b) Although the cleanup of vomit is not considered an activity that falls under the requirements of 1910.1030 unless it contains visible blood, it is recommended that precautions be taken to prevent contact with the materials. This includes the use of personal protective equipment such as gloves and eye protection and a general cleaner to wipe surfaces after the vomit has been removed.

Appendix C: Hepatitis B Vaccine Declination Form

HEPATITIS B VACCINE DECLINATION

SIGNATURE MANDATORY FOR THOSE DECLINING TO BE VACCINATED

I understand that due to my occupational exposure to bloodborne pathogens or other potentially infectious materials I may be at risk of acquiring hepatitis B virus (HBV) infection.

I have been given the opportunity to be vaccinated with hepatitis B vaccine, at no charge to myself. However, I decline hepatitis B vaccination at this time. I understand that by declining this vaccine, I continue to be at risk of acquiring hepatitis B, a serious disease. If in the future I continue to have occupational exposure to blood or other potentially infectious materials and I want to be vaccinated with hepatitis B vaccine, I can receive the vaccination series at no charge to me.

Declining Individual's Name (Print clearly)

Date

Declining Individual's Signature

Social Security Number

**Appendix D: Healthcare Professional's Written Opinion Form for Bloodborne Pathogens
Post Exposure Evaluation and Follow-up**

To:

Date:

Healthcare Professional's Written Opinion for Bloodborne Pathogens Post-Exposure
Evaluation and Follow-up

Employee Name: _____

Job Title: _____ Division: _____

The above named employee has been informed of the results of the post-exposure evaluation on
_____, 20____. Employee has also been told about any medical conditions resulting from
exposure to blood or other potentially infectious materials which require further evaluation or
treatment.

Signature: _____ Date: _____

Healthcare Professional Name: _____

Cc: Employee

Appendix E: Bloodborne Pathogens Training Contents

The Bloodborne Pathogen training module shall include the following topics:

- (1) An accessible copy of the regulatory text of the OSHA Bloodborne Pathogens Standard and an explanation of its contents;
- (2) Epidemiology and symptoms of HIV, HBV, HCV and other bloodborne pathogens;
- (3) Modes of transmission of HIV, HBV, HCV and other bloodborne pathogens;
- (4) A review of the NIST Bloodborne Pathogens Exposure Control Plan;
- (5) Appropriate methods for recognizing tasks and other activities that may involve exposure to blood and other potentially infectious materials;
- (6) An explanation of the use and limitations of methods that will prevent or reduce exposure including appropriate engineering controls, work practices, and personal protective equipment;
- (7) Sharps injury protection;
- (8) Use and limitations of universal precautions, engineering controls, and work practices;
- (9) Types, selection, proper use, location, removal, handling, decontamination and/or disposal of PPE;
- (10) Information on the Hepatitis B vaccine, including its efficacy, safety, method of administration, the benefits of being vaccinated, and that the vaccine and vaccination will be offered to covered employees free of charge;
- (11) Information on the appropriate actions to take and persons to contact in an emergency involving blood or other potentially infectious materials;
- (12) An explanation of the procedure to follow if an exposure incident occurs, including the method of reporting the incident and the medical follow-up that will be made available;
- (13) Discussion of post-exposure evaluation and follow-up;
- (14) Signs and labeling;

991
992 (15) An opportunity for interactive questions and answers with the person conducting the training
993 session; and
994
995 (16) The person conducting the training shall be knowledgeable in the subject matter covered by
996 the elements contained in the training suborder as it relates to the workplace that the training
997 will address.
998
999

Appendix F: Sharps Injury Log

The OSHA Bloodborne Pathogen standard requires that a Sharps Injury Log be maintained to record all contaminated sharps injuries in a facility. The purpose of this log is to help users to evaluate and identify problem devices or procedures that require attention.

Date	Type of Device	Brand Name of Device	Work Area Where Injury Occurred	Brief Description of How the Incident Occurred

CRYOGEN SAFETY

NIST S 7101.52

Effective Date: 04/01/2014

Document Approval Date: 04/30/2013

1. PURPOSE

The Cryogen Safety suborder provides the requirements and guidance to enable employees to work safely with or around cryogenics.

2. BACKGROUND

None.

3. APPLICABILITY

- a. This suborder is limited to the use of liquid helium, liquid nitrogen, liquid neon, and liquid argon and the liquid-to-vapor transition. Since oxygen has the potential to condense, accumulate, and drip from transfer lines when liquid cryogenics with normal boiling points lower than that of oxygen are being transferred, and thereby pose a risk of explosion or fire, its properties are included in this document for reference. Other cryogenics such as liquid hydrogen, liquid ammonia, and numerous other refrigerants may pose hazards that require significantly different controls from those described in this Cryogen Safety suborder. The use of cryogenics other than helium, nitrogen, neon and argon should be brought to the attention of line management for additional review.

4. REFERENCES

- a. ASME Boiler and Pressure Vessel Code Section VIII, Division 1.
- b. ANSI/ASME B31.1, Power Piping.
- c. ANSI/ASME B31.3, Process Piping.
- d. CGA P-12, Safe Handling of Cryogenic Liquids.

- e. NFPA 45, Fire Protection for Laboratories Using Chemicals.
- f. NFPA 55, Standard for the Storage, Use, and Handling of Compressed Gases and Cryogenic Fluids in Portable and Stationary Containers, Cylinders, and Tanks.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.59: Chemical Hazard Communication;
- b. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;
- c. NIST S 7101.22: Hazard Signage;
- d. NIST S 7101.21: Personal Protective Equipment (PPE); and
- e. NIST S 7101.23: Safety Education and Training.

6. REQUIREMENTS

a. General

- (1) The OUs shall manage cryogenic hazards in accordance with NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews, their OU implementations thereof, and the requirements of this suborder.

b. Hazard Analysis

- (1) The hazard analysis process shall encompass cryogenic hazards in all areas where cryogens are used and stored.
- (2) Oxygen-deficiency/oxygen-enrichment hazard assessments must be done as part of the hazard review before beginning any cryogenic experiments. Appendix A of this suborder lists physical characteristics of the most common cryogens, including expansion ratios, which are critical in calculating oxygen-deficiency hazards. Where characteristics are affected by atmospheric pressure, different values are listed for Boulder, CO and Gaithersburg, MD.
 - (a) There are several acceptable methods of determining the risk of ODH available through the Cryogen Safety Program webpage on the NIST safety website.

c. Hazard Control

- (1) Appropriate control measures shall be selected, documented, and implemented.
- (2) Cryogen handling is not permitted in laboratories without adequate ventilation, or, if ventilation is inadequate or non-existent, without additional applied controls that reduce the risk of exposure of personnel to an ODH to an acceptable level.
- (3) Hazard signage that is in accordance with the Hazard Signage Program shall be posted at every entrance to every space that may have an ODH hazard. Example signs are presented in Appendix B of this suborder. The hazard review shall identify the level of hazard, so that the appropriate signal word can be selected for the sign(s). See the Definitions section of this suborder for a description of the various signal words. In most cases, the signal word will either be “DANGER” or “WARNING”.
- (4) When a laboratory cannot reduce the risk of exposure of personnel to an ODH to an acceptable level, the hazard review shall ensure that an oxygen monitor is used. A fixed oxygen monitor shall have an audible alarm, warning light, and a digital readout. Personal monitors may also be used or required depending on the risk.
 - (a) Oxygen monitors shall be installed, used, maintained, and calibrated according to manufacturers’ recommendations.
 - (b) Calibration and maintenance records shall be kept with or near the monitor.
 - (c) The hazard review should consider the need to tie the alarm to a central fire alarm system.
- (5) Cryogen containers that are appropriate for the experiment design, facility, and research activity shall be selected during the hazard review.
 - (a) Glass dewars and cryostats can be used only after they have been specifically addressed in the applicable hazard review.
 - (b) Appropriate Styrofoam containers are permitted for the temporary storage of small amounts of LN₂ if allowed by the hazard review.
 - (c) Regular thermos bottles are not permitted for storing liquid cryogens even for short periods of time.

- (d) Non-pressurized storage dewars shall not be pressurized or modified to be pressurized as these containers are not designed to withstand pressure.
- (e) Hazard reviews shall be conducted before any dewar is modified and subsequently used. All potentially impacted personnel, including storeroom personnel who fill the dewar, shall be included in the hazard review process and/or informed of its results.
- (f) Changes to dewars shall be accomplished by the addition of plumbing or hardware where practical and technically appropriate, rather than the removal of existing hardware and substituting new.
- (g) Adequate pressure-relief devices must be provided throughout the cryogen system to prevent high-pressure gas build-up as the liquid evaporates. For example, a cryostat should have redundant fill tubes or, if not, a burst disk on the vacuum space. Basically, there should always be at least two relief paths for a liquid-containing vessel. This issue needs to be dealt with on a case-by-case basis as part of the hazard review.
- (h) If feasible, existing equipment, systems, and operations shall be brought into compliance with current standards. The safety aspects related to any exceptions to current standards shall be reviewed in detail and documented, and further operation shall be contingent on OU Director's approval.
- (i) Maintenance and inspection requirements for dewars, cryostats, and cryogenic systems shall be developed during the hazard review process and included in the Standard Operating Procedures (SOPs). At a minimum, an initial inspection of the equipment by a trained cryogen user should be conducted before equipment is put into operation.

(6) Transport

- (a) To transport a dewar between floors, use an elevator. Small amounts of cryogen in non-pressurized containers may be carried on stairs with extreme caution and shall be assessed in the OU on a case-by-case basis. Due to the risk of an Oxygen Deficiency Hazard, no one may accompany a dewar in an elevator. Depending on the elevator this may require two people (one at the sending floor and one at the receiving floor), and signage prohibiting anyone from riding the elevator with the dewar. An example sign is included in Appendix B of this suborder. If an elevator allows manual operation using a key, transport may be accomplished without a person at the receiving floor as the elevator will remain in the manual mode (preventing use by

other people) until the operator with the key arrives to remove the dewar and switch it out of manual mode. Signage prohibiting anyone from entering the elevator is recommended in the manual mode.

- (b) Transporting cryogens in vehicles shall only be done by personnel who work in the storeroom, shipping and receiving, a laboratory, or by a contract supplier, and the personnel shall be specifically trained in the proper transport of cryogens. All transports of cryogens must occur in open vehicles, such as pickups or flatbed trucks, and the dewars being transported must be secured. Wheel brakes, if present, must be locked.
- (7) The hazard review or associated SOPs shall describe the required controls to minimize the risks, in accordance with the Chemical Management suborder.
- (a) Safe work practices to minimize the risk of cryogen contact, based on how the cryogen is being used, shall be listed in SOPs. An OU or Division may choose to adopt a set list of safe work practices, such as the cryogen tool titled *Short List of Proper Cryogen Handling Practices*, in order to avoid repetition in multiple hazard reviews and/or SOPs.
- (8) Personal Protection Equipment (PPE) assessments for the use of cryogens shall be completed as part of the hazard review and in accordance with the NIST S 7101.21: Personal Protective Equipment. Some well-defined and controlled tasks may require less PPE, and some operations may need to balance the need for dexterity with PPE requirements. To accommodate these needs, the PPE requirements may be reduced when the reason is documented as part of an approved SOP and hazard review.
- (a) When pouring cryogens from hand-held dewars or transferring liquid cryogens from low-pressure pressurized storage dewars, the following shall be required:
 - i. Eye protection that provides at least as much protection as safety glasses with side shields.
 - ii. Closed toe shoes.
 - iii. Gloves whenever there is risk of exposure to liquid cryogen, cold gas, or cold surfaces, except when the loss of dexterity would present a greater risk. Either approved cryogenic gloves or oil-free leather gloves must be used, and they should be loose enough to allow for rapid removal.

- iv. Protective clothing when there is risk of exposure to the liquid cryogen, such as when transferring from a storage dewar into a smaller cryostat. Either a cryogenic apron or a lab coat with no pockets (to prevent trapping the liquid) should be worn. Clothing should be reviewed for its potential to trap the cryogen before transfer is made.
 - v. Protective clothing when there is a risk of exposure to cold gas during cryogen transfer and when wearing the protective clothing would not present a greater hazard. Simple coverage is often sufficient.
- (b) When transferring cryogens from high-pressure pressurized storage dewars, the PPE required must be specified in the hazard review for each specific experiment.
- (9) Avoid ingestion or inhalation of cryogenic liquid or gas. Under no circumstances should liquid cryogen be put in the mouth as a demonstration, even in small quantities.
- (10) Training and Communication
- (a) Chemical labeling shall be in accordance with the NIST S 7101.59: Chemical Hazard Communication, and hazard signage shall be in accordance with the requirements of the NIST S 7101.22. Appendix B contains sample hazard signage for ODH.
 - (b) Training developed by the OSHE Cryogen Safety Program Manager and the OUs shall be in accordance with the requirements of the NIST S 7101.23: Safety Education and Training and made available for use by employees. The training should include topics such as the following, as appropriate:
 - i. Properties of cryogens in their liquid and gas states;
 - ii. Safe operation of equipment being used with cryogens (i.e., location and function of valves, pressure reading devices, safety devices, inspections, etc.);
 - iii. Equipment hazards/failure modes;
 - iv. Oxygen deficiency risk assessments where cryogens are being used;
 - v. Materials compatible with cryogens (if relevant to the task);
 - vi. Location and use of personal protective equipment (PPE);

- vii. Emergency response; and
 - viii. Situations that cause cryo-pumping and formation of an ice blockage; ice blockage identification; and ice blockage removal techniques or resources.
- (c) Training shall be provided by the OU to all cryogen users during their initial assignment and it shall include hands-on training.

(11) Emergency Procedures

(a) The hazard review shall include emergency procedures for the laboratories.

(b) Situations warranting consideration as appropriate include:

- i. Response to alarms;
- ii. Asphyxiation;
- iii. Frostbite;
- iv. Ice plug;
- v. Tipped container;
- vi. Damaged container;
- vii. Spill;
- viii. Over-pressurization and/or explosion;
- ix. Implosion; and
- x. Embrittlement of materials.

d. Recordkeeping

(1) OU/Division-specific training shall be documented and recorded in accordance with the requirements of the NIST S 7101.23: Safety Education and Training.

- (2) Calibration and maintenance records shall be kept in accordance with OU/Division policies and procedures.

7. DEFINITIONS

- a. Cryogen – A liquid with a normal boiling point below -150 degrees C; applies to either the cryogenic liquid or its gas at or near its boiling point.
- b. Cryostat – A cryogenic vessel configured for low-temperature experiments (as opposed to a dewar which is for storing cryogenics).
- c. Dewar – Vacuum-jacketed vessel designed to store cryogenics. May be of two types:
 - (1) Non-pressurized Storage Dewar – Non-pressurized, vacuum-jacketed vessel with a loose-fitting dust cap over the outlet of the neck tubes, which reduces the chance of atmospheric moisture plugging the neck and allows gas produced from the vaporizing liquid to escape. Depending on the size, liquid is removed by pouring or using a transfer tube. Tubing must be vented to maintain atmospheric pressure and prevent pressurization.
 - (2) Pressurized Storage Dewar – Double-walled vacuum vessel with multilayer insulation in the annular space and equipped with safety-relief valves and rupture discs to protect the vessels from pressure build-up. These containers are categorized as either low-pressure (which can operate at pressures up to about 25 psig) or high-pressure (which can operate at pressures up to 350 psig) liquid containers, with varying capacities. Product may be withdrawn as a gas by passing liquid through the internal vaporizer or as a liquid under its own vapor pressure or an external pressure source.
- d. Emergency – A highly dangerous condition that needs to be addressed immediately, which may be caused by an unplanned or unanticipated occurrence such as equipment failure, a container rupture, or an uncontrolled release of a hazardous chemical into the workplace.
- e. Engineering Controls – Include designing or modifying laboratories, equipment, ventilation systems, and processes to reduce or eliminate the exposure to hazardous sources or conditions. Engineering controls are used to remove a hazard or place a barrier between the worker and the hazard.
- f. Oxygen Deficiency – <19.5% oxygen in air, as defined by OSHA.
- g. Oxygen Enrichment – >23.0% oxygen in air, as defined by OSHA.

- h. Signal Word – A word that designates a degree or level of hazard seriousness.
- (1) “Danger” – Indicates an imminently hazardous situation that, if not avoided, **will** result in death or serious injury.
- (2) “Warning” – Indicates a hazardous situation that, if not avoided, **could** result in death or serious injury.
- (3) “Caution” – Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury.
- (4) “Notice” – The preferred word to address situations not related to personal injury.

8. ACRONYMS

- a. ACGIH – American Conference of Governmental Industrial Hygienists
- b. ANSI – American National Standards Institute
- c. ASME – American Society of Mechanical Engineers
- d. ASTM – American Society of Testing and Materials
- e. CGA – Compressed Gas Association
- f. IDLH – Immediately Dangerous to Life and Health
- g. NFPA – National Fire Protection Association
- h. NIST – National Institute of Standards and Technology
- i. ODH – Oxygen Deficiency Hazard
- j. OSHA – Occupational Safety and Health Administration at the U.S. Department of Labor or state level
- k. PPE – Personal Protective Equipment
- l. SOP – Standard Operating Procedure

9. RESPONSIBILITIES

- a. The OUs are responsible for ensuring that the requirements in Section 6 are met.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

- a. Appendix A. Cryogen Properties
- b. Appendix B. Hazard Signage

Appendix A. Cryogen Properties

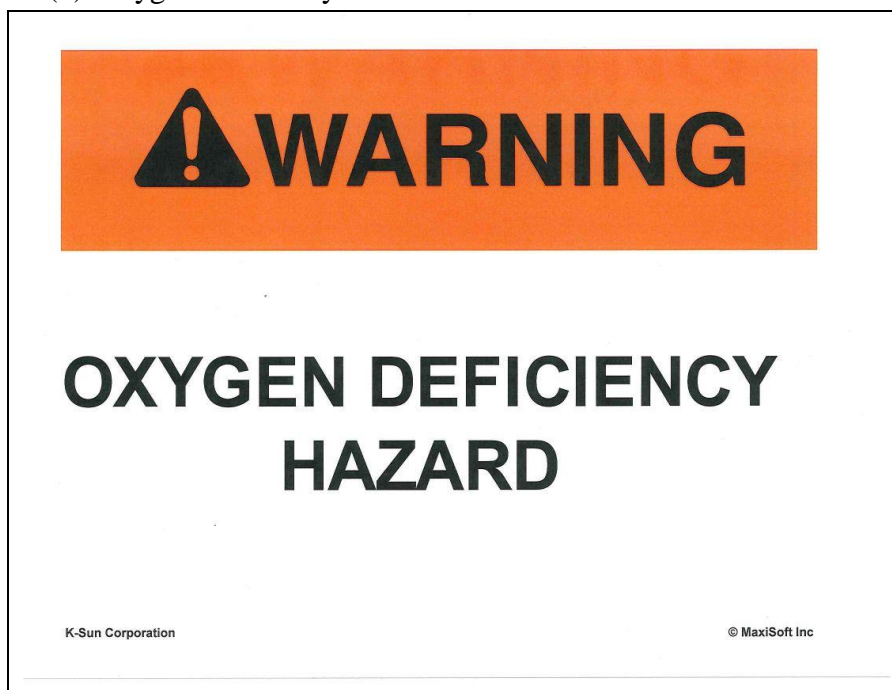
Table 1 reflects a partial list of properties for the cryogens included in this suborder, namely, helium, nitrogen, neon, and argon. In addition, since oxygen has the potential to condense on surfaces cooled by cryogens with normal boiling points lower than that of oxygen, thereby posing a risk of explosion or fire, its properties are included here for reference.

Table 1: Properties of common cryogens

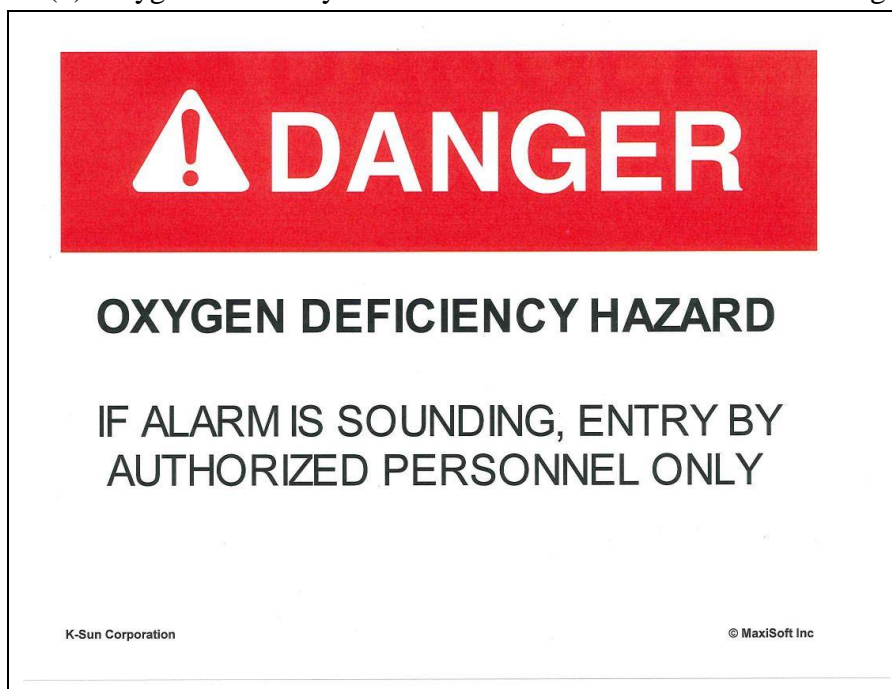
		Helium		Neon		Nitrogen		Argon		Oxygen	
Boiling Point (K)	@Sea level, 101.325 kPa (1atm)	4.2		27.1		77.3		87.3		90.2	
Liquid Density (g/L)	@Sea level, 101.325 kPa (1atm)	125		1207		806		1395		1141	
	Location	273K	293K	273K	293K	273K	293K	273K	293K	273K	293K
Gas Density (g/L)	Boulder	0.15	0.14	0.77	0.72	1.07	1.00	1.53	1.43	1.23	1.14
	Gaithersburg	0.18	0.17	0.90	0.84	1.25	1.17	1.78	1.66	1.43	1.33
Gas/liquid Expansion Ratio (from liquid to gas, local atm)	Boulder	813	873	1561	1676	751	806	911	978	930	998
	Gaithersburg	698	750	1341	1439	644	692	782	839	798	857

Appendix B. Hazard Signage

(1) Oxygen deficiency hazard



(2) Oxygen deficiency hazard – Do not enter if alarm is sounding



(3) Do Not Enter Elevator



(4) Suffocation (Asphyxiation) Warning Symbol



(5) Cold Warning Symbol



Magnetic Field Safety

NIST S 7101.53

Document Approval Date: 02/15/2013

Effective Date: 04/01/2014

1. PURPOSE

The National Institute of Standards and Technology (NIST) Magnetic Field Safety Program has been developed to reduce the risk of exposure to magnetic fields in excess of the recommended exposure limits. The primary objective of the NIST Magnetic Field Safety program is to provide guidance for NIST employees on control measures, exposure limits, hazard signage, and training for working with and in the vicinity of magnetic fields.

2. BACKGROUND

None.

3. APPLICABILITY

- a. The provisions of this program apply to all NIST facilities and to all NIST employees who work with and around devices and equipment designed to generate magnetic fields, both static and time varying with frequencies up to 30 kilohertz (kHz) with the exceptions noted in [NIST O 710.01](#), Occupational Safety and Health Order.

4. REFERENCES

- a. 29 CFR 1910.97, Occupational Safety and Health Administration, Non-Ionizing Radiation.
- b. 47 CFR 1.1307(b), Environmental Assessments.
- c. *TLVs and BEIs based on the Documentation of the Threshold Limit Values for Chemical Substances and Physical Agents and Biological Exposure Indices*, American Conference of Governmental Industrial Hygienists (current edition).

- d. *Guidelines on Limits of Exposure to Static Magnetic Fields*, International Commission on Non-Ionizing Radiation Protection (2009).
- e. *Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields (Up to 300 GHz)*, International Commission on Non-Ionizing Radiation Protection (1998).

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.52: Cryogen Safety;
- b. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;
- c. NIST S 7101.22: Hazard Signage;
- d. NIST S 7101.24: Incident Reporting and Investigation; and
- e. NIST S 7101.23: Safety Education and Training

6. REQUIREMENTS

- a. General Magnetic Field Safety Requirements

(1) This section describes the basics of magnetic field safety, biological effects, and exposure limits to be used at NIST.

(2) Since there are varying types of magnetic field sources and numerous equipment configurations, the general approach to safety is to define the quantities that must be measured, and follow established limits on the values to assure that no adverse health effects will occur.

(3) Magnetic field hazards shall be managed in accordance with NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews, Organizational Unit implementations thereof, and the requirements of this program.

- b. Program Categories

(1) Although both static and time-varying magnetic fields and associated electromagnetic fields are not known to cause apparent long-term health effects, there are hazards, under

some circumstances that need to be recognized and controlled to avoid accidents or injury.

(2) All equipment capable of generating magnetic fields that may exceed the recommended exposure limits established for the general workplace of 2T (20,000 G) at accessible areas, should be inventoried, appropriately labeled, and used only by authorized/trained personnel.

(3) Exposure limits for magnetic fields and requirements for engineering and administrative controls are listed in the following subsections.

c. Static and Time-Varying Fields up to 30 kHz

(1) General

(a) The primary safety concern with exposure to static and time-varying magnetic fields is the attraction of magnetic objects in or on the body in an external magnetic field gradient that could lead to a “missile effect” or striking hazard, injuring body tissue. Additionally, magnetic objects may rotate in a magnetic field, which could result in the tearing of body tissue. Exposure to a static magnetic field may temporarily reprogram cardiac pacemakers and inhibit implantable cardioverter-defibrillators.

(2) Exposure Limits for Static Magnetic Fields

(a) TLVs recommended by the ACGIH and by the International Commission on Non-Ionizing Radiation Protection (ICNIRP) will be followed at NIST as consensus standards for employee protection. These TLVs are based on an assessment of available data from laboratory research and human exposure studies. Table 1 provides the TLVs for static magnetic fields.

(b) Routine occupational exposures to static magnetic fields should not exceed 2 T (20,000 G) in the general workplace but can have ceiling values up to 8 T (80,000 G) in a controlled area. See Table 1.

Table 1. Recommended Limits of Exposure to Static Magnetic Fields

[For reference, see Sections 3d (2011 edition) and 3e.]

Exposure Characteristics	Magnetic Flux Density (Ceiling Value)
Whole body (General workplace)	< 2 T (20,000 G)
Whole body (Controlled area)	2-8 T (20,000-80,000 G)
Limbs	20 T (200,000 G)
Medical device wearers	0.5 mT (5 G)
General public*	400 mT (4,000 G)

Note: While SI is the adopted method of units used at NIST, cgs units of Gauss (G) are included for the convenience of the staff.

*Note: The ACGIH does not have an exposure limit for the general public. This value was taken from *Guidelines on Limits of Exposure to Static Magnetic Fields*, ICNIRP (2009).

(3) Exposure Limits for Time-Varying Magnetic Fields with Frequencies (f) in the range 0 Hz < f < 1 Hz

(a) Time-varying magnetic fields with frequencies in this range are considered, for the purposes of this suborder, to be static fields. The recommended limits of exposure provided in Table 1 apply.

(4) Exposure Limits for Time-Varying Magnetic Fields from 1 to 30 kHz.

(b) TLVs for time-varying magnetic fields recommended by the ACGIH will be followed at NIST as consensus standards for employee protection.

(c) The TLVs in Table 2 refer to the amplitude of the magnetic flux density (B) of sub-radiofrequency (sub-RF) magnetic fields at frequencies (f) in the range of 1 to 30 kHz to which it is believed that nearly all workers can be exposed repeatedly without adverse health effects. The magnetic field strengths in these TLVs are root-mean-square values.

Table 2. Limits of Exposure to Time-Varying Magnetic Fields

[For reference, see Sections 3d (2011 edition) and 3e.]

Exposure Characteristics		Magnetic Flux Density (Ceiling Value)
1 Hz to 300 Hz	Whole body	$(60 / f)$ mT
	Arms and legs	$(300 / f)$ mT
	Hands and feet	$(600 / f)$ mT
300 Hz to 30 kHz	Whole body and partial body	0.2 mT
50 / 60 Hz	Individuals having implanted pacemakers	0.1 mT

Note: $1 \text{ mT} = 10 \text{ G}$; f in Hz

(5) Requirements for Engineering and Administrative Controls

- (a) All areas where individuals could be exposed to magnetic fields that exceed or could exceed 0.5 mT (5G) for static magnetic fields or 0.1 mT (1 G) for time-varying magnetic fields shall be surveyed to establish appropriate safety limits; postings, including hazard signage (refer to Appendix A for examples of hazard signs); and barriers. The Magnetic Field Safety Program Manager can assist with these measurements.
- (b) A “Danger” sign (imminent threat to life or health) shall be posted at every entrance or access point to any laboratory or facility where exposure to magnetic fields may exceed the recommended medical-device-wearer exposure limits of 0.5 mT (5G) for static magnetic fields or 0.1 mT (1 G) for time-varying magnetic fields. Medical-device wearers shall not be exposed to fields in excess of the medical-device-wearer exposure limits.
- (c) A “Danger” sign (imminent threat to life or health) shall be posted at every entrance or access point to any laboratory or facility where exposures to static magnetic fields may exceed the recommended medical-device-wearer exposure limits of 0.5 mT (5 G) for static magnetic fields or 0.1 mT (1 G) for time-varying magnetic fields and where static magnetic fields – or time varying magnetic fields with frequencies below 1 Hz – could exceed the general workplace limit of 400 mT (4,000 G).

(d) A “Danger” sign (imminent threat to life or health) shall be posted at every entrance or access point to any laboratory or facility where exposures to magnetic fields may exceed the recommended medical-device-wearer exposure limits of 0.5 mT (5G) for static magnetic fields or 0.1 mT (1 G) for time-varying magnetic fields and where static magnetic fields – or time-varying magnetic fields with frequencies below 1 Hz – could exceed the general workplace exposure limit of 2 T (20,000 G), in which case access is limited to trained workers (see Section 6e). In addition to posting the hazard sign at the entrance, it is recommended that around the magnet where general workplace exposure limits of 2 T (20,000 G) may be exceeded, a line be painted or taped on the floor or a physical barrier such as a plastic chain or rope be used to mark the exposure area. This is not necessary if the laboratory serves as the controlled area and is identified as such on a sign posted at the entrance. Other engineering or administrative controls can also be used after consulting with the Magnetic Field Safety Program Manager.

(e) A general magnetic field warning label should be posted on any device capable of producing external magnetic fields in excess of the recommended general workplace exposure limit of 2T (20,000 G).

d. Special Considerations – Use of Cryogenic Liquids to Cool Magnets or Associated Equipment

(1) Because of the very low temperature of cryogenic liquids, contact can produce frostbite or cold burns. Unprotected skin that comes into contact with non-insulated items of the cold equipment may become stuck and the skin may be torn on removal.

(2) When a magnet quenches, the loss of magnetic field and sudden boil-off of cryogenic coolant can pose a significant safety risk. The released gases displace oxygen in the air, and this can cause rapid asphyxiation and unconsciousness without warning.

(3) When working with cryogenic liquids, follow procedures specified in the NIST Cryogen Safety Program.

e. Training and Recordkeeping

(1) Training on the NIST Magnetic Field Safety Suborder is required for NIST supervisory and line management personnel of employees working in areas where exposures to static magnetic fields – or time-varying magnetic fields with frequencies below 1 Hz – could exceed the general workplace limit of 2 T (20,000 G), to any part of the body.

(2) Training on Magnetic Field Safety is required for employees working in areas where exposures to static magnetic fields – or time-varying magnetic fields with frequencies below 1 Hz – could exceed the general workplace limit of 2 T (20,000 G) to any part of the body.

(3) Training on this program and pertinent OU/division policies and procedures shall be provided, documented, and recorded in accordance with requirements of the NIST Safety Education and Training Program.

7. DEFINITIONS

- a. Administrative Controls – Controls that alter the way work is done, including timing of work, policies, training, and other rules.
- b. Authorized personnel – NIST employees who could be exposed to magnetic fields above 2 T (20,000 G) to any part of the body and have successfully completed the required Magnetic Field Safety Training.
- c. B Field – Magnetic flux density or magnetic induction. Units are tesla (T) and gauss (G).
- d. Controlled Area – An area where exposures of personnel to magnetic fields may exceed 2 T (20,000 G) and to which access is limited to trained workers.
- e. E Field – Electric field strength, measured in units of volts per meter (V/m).
- f. Engineering Controls – Controls that Include designing or modifying laboratories, equipment, ventilation systems, and processes to reduce or eliminate the exposure to hazardous sources or conditions. Engineering controls are used to remove a hazard or place a barrier between the worker and the hazard.
- g. Exposure Limit – Value to which an individual may be exposed without harmful effects and with an acceptable safety factor.
- h. General Public – For the purposes of this suborder, NIST visitors, i.e., individuals on a NIST site or in a NIST facility who are neither NIST employees nor NIST associates.
- i. H Field – Magnetic field strength, measured in units of amps per meter (A/m).
- j. Hertz – The oscillation frequency of the electromagnetic field in cycles per second (Hz).

- k. Magnetic Field – A field (H field) created by a magnet or as a consequence of the movement of electric charges. Its intensity is measured in units of A/m.
- l. Non-ionizing Radiation – Radiation in the part of the electromagnetic spectrum where there is insufficient energy to cause ionization. It includes electric and magnetic fields, radio waves, microwaves, infrared, ultraviolet and visible radiation.
- m. Occupational Exposure – Exposure of individuals to non-ionizing radiation as a consequence of their employment, who have been made aware of the potential of exposure, and who can exercise control over their exposure through the use of administrative or engineering controls or safe work practices.
- n. Quenching – Process in which the coil of a superconducting magnet reverts to a resistive state, which results in loss of magnetic field and a rapid boil-off of the cryogenic coolant.
- o. Signal word "Danger" – Indicates an imminently hazardous situation that, if not avoided, **will** result in death or serious injury.
- p. Signal word, "Caution" – Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury.
- q. Signal word, "Notice" – The preferred word to address situations not related to personal injury.
- r. Signal word, "Warning" – Indicates a hazardous situation that, if not avoided, **could** result in death or serious injury.
- s. Static Magnetic Field – Field that varies at frequencies below 1 Hz and is created by either a permanent magnet or a direct-current electromagnet.
- t. Time-Varying Magnetic Field – Field produced by alternating currents of frequencies up to 30 kHz.
- u. Threshold Limit Value (TLV) – An occupational limit that workers may be exposed to repeatedly without adverse health effects. TLVs are published by the American Conference of Governmental Industrial Hygienists (ACGIH).
- v. Whole-Body Exposure – Exposure of the head, trunk, arms above the elbow, and/or legs above the knee.

288 **8. ACRONYMS**

- 289 a. ACGIH – American Conference of Governmental Industrial Hygienists
290
291 b. BEI – Biological Exposure Indices
292
293 c. CFR – Code of Federal Regulations
294
295 d. ICNIRP – International Commission on Non-Ionizing Radiation Protection
296
297 e. IEEE – Institute of Electrical and Electronics Engineers
298
299 f. MPE – Maximum Permissible Exposure
300
301 g. NIOSH – National Institute for Occupational Safety and Health
302
303 h. NIST – National Institute of Standards and Technology
304
305 i. TLV – Threshold Limit Value
306
307

308 **9. RESPONSIBILITIES**

- 309 a. The OUs are responsible for ensuring that the requirements in Section 6 are met.
310
311

312 **10. AUTHORITIES**

313 There are no authorities specific to this suborder alone.
314
315

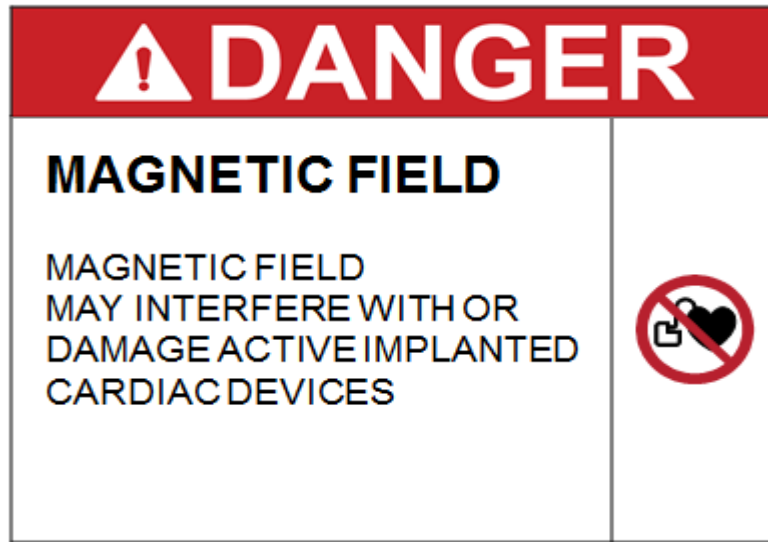
316 **11. DIRECTIVE OWNER**

317 Chief Safety Officer
318
319

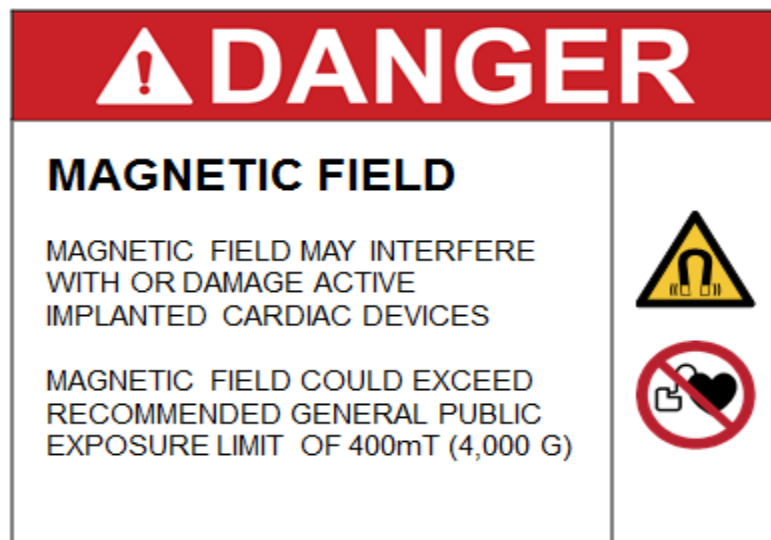
320 **12. APPENDICES**

- 321 a. Appendix A. Magnetic Field Hazard Signage
322
323
324
325
326
327

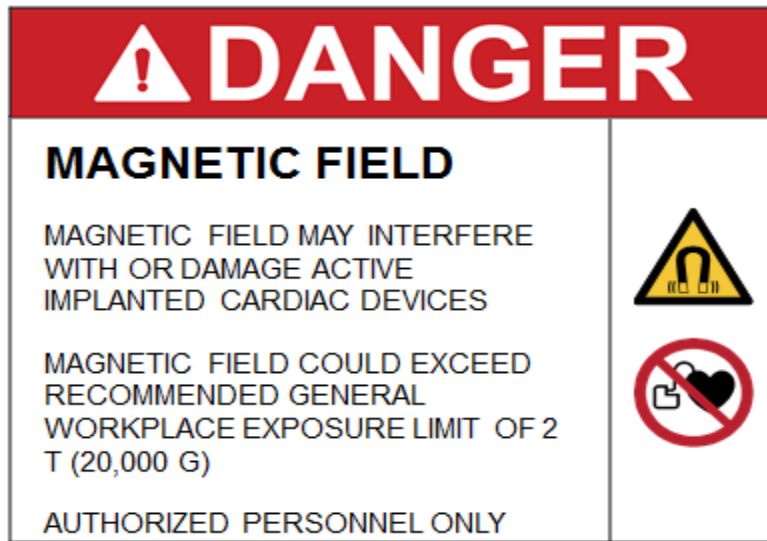
Appendix A. Magnetic Field Hazard Signage



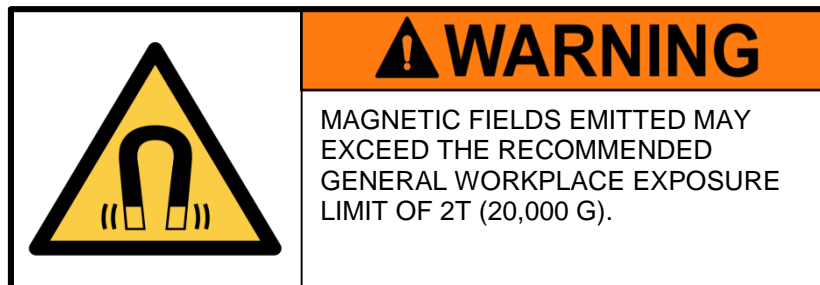
- a. Danger Sign– Magnetic Field May Interfere with or Damage Implanted Cardiac/Medical Devices.



- b. Danger Sign- Magnetic Fields May Interfere with or Damage Implanted Cardiac/Medical Devices and Could Exceed the Recommended General Public Exposure Limits.



- c. Danger Sign – Magnetic Fields May Interfere with or Damage Implanted Cardiac/Medical Devices and Could Exceed the Recommended General Workplace Exposure Limits.



- d. Warning Label - Device capable of producing external magnetic fields in excess of the recommended general workplace exposure limit of 2T (20,000 G).

Dispersible Engineered Nanomaterials

NIST S 7101.54

Document Approval Date: 04/18/14

Effective Date: 04/01/2016

1. PURPOSE

The purpose of the NIST DENMs Program is to eliminate or minimize occupational exposure to DENMs and to make NIST employees and associates aware of the potential airborne and dermal hazards associated with exposure.¹

2. BACKGROUND

This suborder supersedes NIST Health and Safety Instruction (HSI) 23, Handling of Dispersible Engineered Nanomaterials, May 2009.

3. APPLICABILITY

This suborder applies to all NIST facilities and to all NIST employees and associates who work with DENMs unless an authoritative government entity (*e.g.*, OSHA, EPA, or NIOSH) has published information confirming that a particular DENM is not hazardous.

4. REFERENCES

- a. General Safe Practices for Working with Engineered Nanomaterials in Research Laboratories, Department of Health and Human Services (DHHS) [National Institute for Occupational Safety and Health (NIOSH)] Publication Number 2012-147.
- b. Current Intelligence Bulletin 63: Occupational Exposure to Titanium Dioxide DHHS (NIOSH) Publication 2011-160.
- c. Current Intelligence Bulletin 65: Occupational Exposure to Carbon Nanotubes and Nanofibers, DHHS (NIOSH) Publication Number 2013-145.

¹ Terms are defined in Section 7; acronyms are defined in Section 8.

- d. Approaches to Safe Nanotechnology: Managing the Health and Safety Concerns Associated with Engineered Nanomaterials, DHHS (NIOSH) Publication Number 2009-125.
- e. Safe Nanotechnology in the Workplace, DHHS (NIOSH) Publication Number 2008-112.
- f. U.S. Environmental Protection Agency: Nanotechnology White Paper, EPA 100/B-07/001, February 2007.
- g. American National Standard, Occupational and Educational Eye and Face Protection, ANSI Z87.1-1989 (or more recent version).

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews
- b. NIST S 7101.21: Personal Protective Equipment;
- c. NIST S 7101.58: Respiratory Protection;
- d. NIST S 7101.59: Chemical Hazard Communication; and
- e. NIST S 7101.22: Hazard Signage.

6. REQUIREMENTS

Using DENMs at NIST requires OUs to be aware of their potential hazards and to provide their employees and associates with a workplace free from the recognized hazards.

These elements entail identification of potential hazards, implementation of engineering and administrative controls, guidance on the selection of PPE, and training.

a. Hazard Review Process

(1) DENMs shall be identified prior to commencement of new processes and changes to existing processes in the work area.

(2) The hazard review process shall include the following considerations to minimize the hazards of and the possibility of exposure to DENMs:

(a) Selection of DENM forms, quantities, and processes;

- 77 i. DENMs used in dry (e.g., powder) form, embedded in solid materials, or
78 suspended in liquids all have the potential to become airborne and inhaled,
79 depending on how they are used. Processes involving, but not limited to, the
80 following have the potential to result in airborne DENMs in the surrounding
81 environment:
- 82
- 83 (i) The use of dry DENMs or DENM-containing dry materials;
- 84
- 85 (ii) The abrading, cutting, cleaving, breaking, or crushing of DENM-containing
86 solid materials;
- 87
- 88 (iii) The intentional or unintentional aerosolization of DENM-containing liquids;
89 or
- 90
- 91 (iv) The production or handling of DENM-containing byproducts, such as those
92 resulting from the evaporation of DENM-containing liquids.
- 93
- 94 (b) All routes of possible exposure to DENMs, including inhalation, ingestion, injection,
95 and dermal contact (including eye and other mucus membranes);
- 96
- 97 (c) The properties of the precursor materials as well as those of the resulting
98 nanomaterial product; and
- 99
- 100 (d) The need for DENM-specific spill-containment and cleanup equipment and
101 procedures.
- 102
- 103 (3) If the hazard review process identifies a potential exposure to DENMs, then a
104 consultation should be scheduled with a competent person to perform an exposure
105 assessment, including exposure monitoring, if warranted, and to advise on the
106 applicability of the requirements of this suborder as needed.
- 107
- 108 b. Engineering Controls
- 109
- 110 (1) Processes capable of generating airborne DENMs shall be conducted in a recirculating
111 hood equipped with HEPA or ULPA or a chemical fume hood, ideally equipped with
112 HEPA or ULPA.
- 113

(a) Laminar-flow clean benches should not be used for DENMs, as these systems are designed for product protection, as opposed to user protection.²

(2) Hoods shall be under negative air pressure with respect to the rest of the laboratory space.

(3) Hoods shall be serviced, maintained, and performance tested in accordance with manufacturers' instructions.

(4) In the event that the face velocity on a hood falls outside the range of face velocities specified by the manufacturer, e.g., as indicated by a hood-flow-monitor alarm, work shall stop until the face velocity has been restored to the specified range.

c. Administrative and Work Practice Controls

(a) Upon receipt, packages containing DENMs shall be opened and inspected within a recirculating hood equipped with HEPA or ULPA or a chemical fume hood, ideally equipped with HEPA or ULPA;

(2) When not in use, all forms of DENMs shall be in tightly-closed, chemically-compatible containers³.

(3) All DENMs shall be segregated and stored according to the hazards associated with constituent chemical properties.

(4) All working surfaces (e.g., benches, glassware, apparatus, exhaust hoods, support equipment) shall be maintained as free as possible of DENM contamination.

(5) Surfaces on which DENMs might settle shall be wiped with a moistened towel or wipe, which shall be disposed of as hazardous waste (see below).

(6) Wet wiping or a dedicated HEPA vacuum shall be used for cleaning DENMs in dry form.

(a) Dry sweeping and the use of compressed air is prohibited.

d. Selection of PPE

(1) PPE selection shall be based on the NIST hazard review process and be in accordance with the requirements of the NIST PPE Program.

² If it is necessary to conduct work using a laminar-flow clean bench, schedule a consultation with the OSHE DENM Program Manager.

³ If DENMs have the potential to react and pressurize a closed container, consult with the DENM Program Manager on obtaining an appropriate container.

(a) Hand protection, when required by the hazard review, shall take into account the properties of the DENMS, the properties of any associated chemicals to be used, and the properties of any byproducts that may result from reactions of the DENMs and associated chemicals.

(b) Eye and face protection, when required by the hazard review, shall, at a minimum, consist of ANSI Z87-compliant safety glasses.

i. Higher levels of eye protection may be necessary depending on the process and type of DENM being used. For example, safety goggles may be required when working with DENMs in liquid form with a potential to aerosolize and enter workers' eyes.

(c) Air-purifying respirators, when required by the hazard review, shall be equipped with a minimum of a P-100 filter.

e. Medical Evaluation

Employees and associates involved in incidents resulting in exposure to DENMs should have a post-incident evaluation conducted and documented by a medical professional.

f. Waste Disposal

Materials contaminated with DENMs, including PPE (e.g., used gloves), cleaning fluids, used HEPA filters, and wipes, shall be placed in sealable, labeled waste containers and disposed of as hazardous waste.⁴

g. Spill Response

(1) General

(a) The spill clean-up procedure below shall be followed if a spill of DENMs occurs and the personnel involved are familiar with the hazards of the spilled material and are confident they can safely control the hazards. Otherwise, the spill shall be reported immediately by calling the Safety Assistance Center at x5375, Option 3.

(2) Spill Clean-Up Procedure

(a) Remove all ignition sources, if possible;

(b) Contain the spill;

⁴ Waste disposal procedures and containers can be obtained by calling the Safety Assistance Center at x5375, Option 3.

- (c) Before selecting a cleaning method, consider the physical and chemical properties of the DENMs and potential reactions with cleaning materials and equipment (e.g., vacuum cleaner filters and canisters);
- (d) If it is necessary to vacuum dry DENMs, ensure that a HEPA vacuum is used and that precautions are taken when changing the filter and/or emptying the vacuum to ensure that DENM's are not reintroduced into the work area;
- (e) Dispose of the spill clean-up materials as hazardous waste; and
- (f) Prohibit re-entry of the work area until it has been cleared for occupancy..

h. Hazard Signage

If an authoritative government entity has published evidence that a DENM is potentially hazardous, then specific hazard signage with the signal word "**Caution**" shall be posted where the DENMs will be handled (e.g., on recirculating or chemical fume hoods). See Appendix A for example signage.

i. Training

Training provided by OSHE on the DENMs program and activity-specific training required by applicable hazard reviews shall be assigned and documented, and its completion by affected employees and associates recorded in accordance with the requirements, roles and responsibilities of the NIST Safety Education and Training suborder.

j. Records of Hazard Assessments

The results of the exposure assessments conducted by competent persons shall be noted, referenced, or included in the activity-hazard-review documentation.

7. DEFINITIONS

- a. Competent Person – A CIH, CSP, or CHMM in the NIST Office of Safety, Health and Environment (OSHE) or another NIST Organizational Unit (OU), a consultant CIH, CSP or CHMM, or an individual directed by a CIH, CSP, or CHMM capable of anticipating, recognizing, controlling, and evaluating potential occupational hazards.
- b. Certified Industrial Hygienist (CIH) – An individual who is board certified by the American Board of Industrial Hygiene and has met the minimum requirements for education, experience, and through examination has demonstrated a minimum level of knowledge in occupational health subject areas such as potential nanotechnology hazards.

- c. Certified Hazardous Materials Manager (CHMM) – An individual who is board certified by the Institute of Hazardous Materials Management and has met the professional challenge of illustrating competency through education, experience, and examination.
- d. Certified Safety Professional (CSP) – An individual who is board certified by the Board of Certified Safety Professionals and has met the professional challenge of illustrating competency through education, experience, and examination.
- e. Dispersible Engineered Nanomaterials (DENMs) – Intentionally-produced materials with one or more dimensions between approximately 1 nm and 100 nm that can be dispersed into (or onto) liquid or solid compounds or aerosolized (suspended in a gas).
- f. Engineered Nanomaterials (ENMs) – Intentionally-produced materials with one or more dimensions between approximately 1 nm and 100 nm;
- g. Engineered Nanoparticles (ENPs) – Intentionally-produced, dispersible particles with two or three dimensions between approximately 1 nm and 100 nm;
- h. High-Efficiency Particulate Air (HEPA) Filter – A filter that is at least 99.97% efficient in removing particles 0.3 micrometers in diameter or greater passing through the filter.
- i. HEPA vacuum – A vacuum which has been designed with a HEPA filter as the last filtration stage and includes a description of what the term HEPA means. The HEPA vacuum must be designed so that all the air drawn into the machine is expelled through the filter.
- j. Shall/Should/May –
- (1) Shall (Must or Will): Indicates that the performance of an item is mandatory.
- (2) Should: Indicates that the performance of an item is not mandatory, but the full implications of not performing that item must be understood and either justified or carefully weighed before choosing a different course.
- (3) May: Indicates that the performance of an item is at the discretion of the individual responsible for the action.
- k. Ultra-Low Particulate Air (ULPA) Filter – A filter that is at least 99.9995% efficient in removing particles or particles of 0.12 micrometers in diameter or greater passing through the filter.

1. Work Area – For the purposes of this suborder, a defined space in a workplace where DENMs are produced or used to which there is a reasonable likelihood that workers present in the space could be exposed.

8. ACRONYMS

- a. CIH – Certified Industrial Hygienist
- b. CHMM – Certified Hazardous Materials Manager
- c. CSP – Certified Safety Professional
- d. CSO – Chief Safety Officer
- e. DENMs – Dispersible Engineered Nanomaterials
- f. DHHS – Department of Health and Human Services
- g. HEPA – High-Efficiency Particulate Air Filter
- h. NIOSH – National Institute for Occupational Safety and Health
- i. PPE – Personal Protective Equipment
- j. OSHE – Office of Safety, Health and Environment
- k. OU – Organizational Unit
- l. ULPA – Ultra-Low Particulate Air Filter

9. RESPONSIBILITIES

- a. The OUs are responsible for ensuring that the requirements in Section 6 are met.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

310 **11. DIRECTIVE OWNER**

311 Chief Safety Officer

312

313

314 **12. APPENDICES**

315 a. Appendix A. Example Hazard Signage

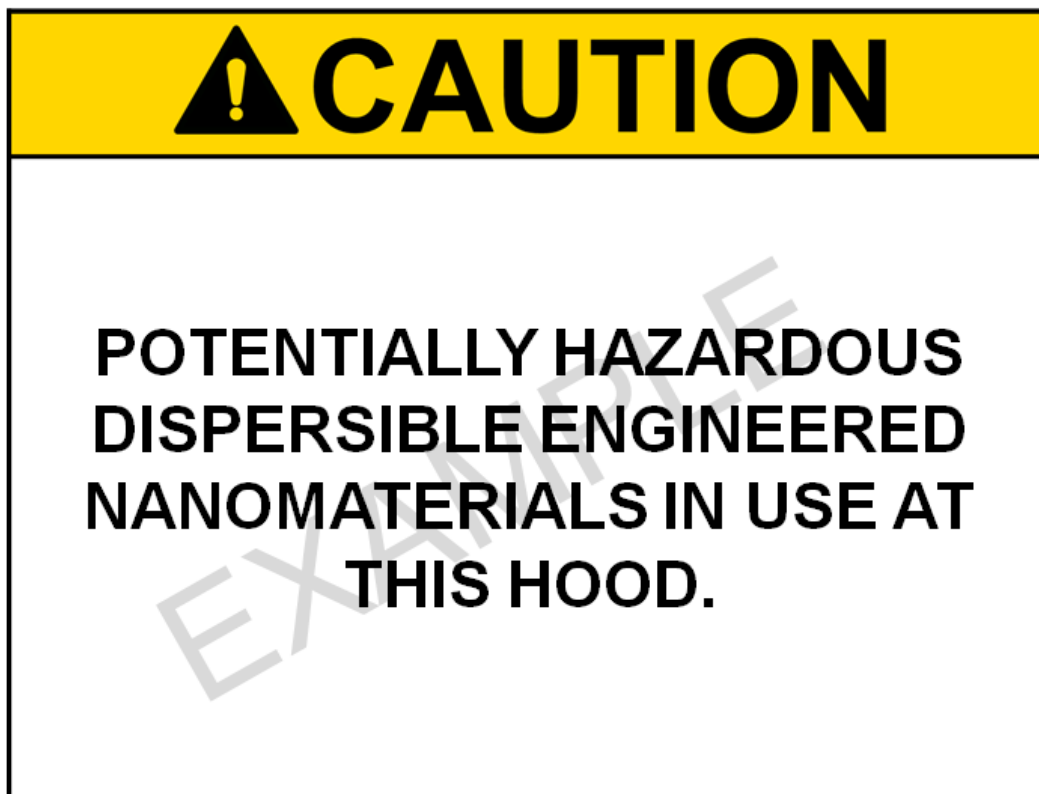
316

317

318

319
320

Appendix A. Revision History



321
322
323
324

HEARING PROTECTION

NIST S 7101.55

Document Approval Date¹: 02/06/2015

Effective Date: 04/01/2015

1. PURPOSE

The purpose of the NIST Hearing Protection Program (HPP) is to reduce the risk of occupational hearing loss through recognition, evaluation, and control of workplace noise-related hazards.

2. BACKGROUND

- a. NIST must meet or exceed the requirements established by OSHA in [29 Code of Federal Regulations \(CFR\) 1910.95](#), Occupational Noise Exposure. Implementation of this suborder through the requirements in Section 6 and the roles and responsibilities in Section 9 exceeds those requirements.
- b. This suborder supersedes NIST Health and Safety Instruction (HSI) 4, Hearing Conservation Program, March 1992.

3. APPLICABILITY

This suborder applies to NIST employees and associates who, in the conduct of their official duties, could receive noise doses that equal or exceed NIST noise dose limits, defined in Section 6a. It also addresses nuisance noise, defined in Section 7.

4. REFERENCES

- a. [29 CFR 1910.95](#), Occupational Noise Exposure
- b. [29 CFR 1904.10](#), Recording of Cases Involving Occupational Hearing Loss

¹ The revision history for this document can be found in Appendix A.

- c. American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Values: Documentation of the Threshold Limit Values for Physical Agents, 2001, 7th Ed.
- d. Criteria for a Recommended Standard, Occupational Noise Exposure; Department of Health and Human Services [National Institute for Occupational Safety and Health (NIOSH)] Publication Number 98-126
- e. American National Standard, Acoustical Terminology, American National Standards Institute (ANSI) S1.1-1994 (R2004)
- f. American National Standard, Specification for Sound-Level Meters, ANSI S1.4-1983 (R2006)/ANSI S1.4A-1985 (R2006)
- g. [OSHA Publication 3074](#), "Hearing Conservation," revised edition, 2002

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;
- b. NIST S 7101.21: Personal Protective Equipment;
- c. NIST S 7101.23: Safety Education and Training; and
- d. NIST S 7101.22: Hazard Signage.

6. REQUIREMENTS²

Requirements include the specification of NIST noise dose limits; hazard identification; hazard assessment; control methods, including hearing protection devices (HPDs) selected by competent persons; use of HPDs; audiometric testing; re-review of activity hazard reviews; training; noise-monitoring records; communication; and buy-quiet initiative, all implemented to ensure that employees and associates do not receive noise doses that equal or exceed NIST noise dose limits. In essence, if potential noise doses equal or exceed NIST noise dose limits, engineering or administrative controls must be implemented. If such controls fail to reduce potential noise doses to less than NIST noise dose limits, HPDs must be provided and used to reduce potential noise doses to less than NIST noise dose limits.³

² The requirements in this section apply to employees and associates who, in the conduct of their official duties, could receive noise doses that equal or exceed NIST noise dose limits, and their management.

³ The requirements delineated below for noise doses that equal or exceed NIST noise dose limits, augmented by the responsibilities in Section 9, constitute NIST's Hearing Conservation Program. NIST's Hearing Conservation Program is more protective than that specified by OSHA in 29 CFR 1910.95(c), Hearing Conservation Program.

a. NIST Noise Dose Limits

- (1) Unprotected employees and associates shall not be exposed, during a work day, to noise levels above 80 dBA for durations that would result in their receiving noise doses, D, that equal or exceed 100%, where D is calculated from:

$$D = [(C_1/T_1) + (C_2/T_2) + \dots + (C_n/T_n)] \times 100\%.$$

Here, C_i is the total exposure time, during a work day, at a specified noise level L_i (≥ 80 dBA), and T_i is the time exposure limit at that noise level calculated from the following equations:

$$T = 8 / 2^{(L - 85)/5} \text{ for } 80 \leq L < 85$$

$$T = 8 / 2^{(L - 85)/3} \text{ for } L \geq 85,$$

with L measured on the A-scale of a standard sound-level meter set at SLOW response and T measured in hours.⁴ Use of these equations yields the following time exposure limits, T , at different sounds levels, L :

L (dBA)	T (h)
80	16
81	13.93
82	12.13
83	10.56
84	9.19
85	8
86	6.35
87	5.04
88	4
89	3.17
90	2.52
91	2
92	1.59
93	1.26
94	1

⁴ The equation for $L > 85$ dBA corresponds to that for the time exposure limits established by ACGIH. The equation for $80 \text{ dBA} \leq L < 85 \text{ dBA}$ corresponds to that for the action levels established by OSHA in 29 CFR 1910.95(c). Its use in that range, rather than the equation for $L \geq 85$ dBA, is necessary to ensure compliance by NIST with the requirements of 29 CFR 1910.95(c) for exposure times greater than 8 hours.

97	0.5
100	0.25
103	0.13
106	0.06
109	0.03
112	0.02
...	...

- (2) Protected employees and associates shall not be exposed to noise levels that would result in their receiving noise doses that equal or exceed 100%, taking into account the attenuation provided by the use of HPDs.

b. Hazard Identification

- (1) If a concern arises⁵ regarding potential noise hazards in an already ongoing activity, a consultation shall be scheduled as soon as possible with a competent person to determine if noise doses could equal or exceed 100%.⁶
- (2) If the hazard review of a new activity identifies potential noise hazards, a consultation shall be scheduled with a competent person to determine if noise doses could equal or exceed 100%.
- (3) If the hazard review of a change in an existing activity identifies new noise hazards or potential increases in previously identified noise hazards, a consultation shall be scheduled with a competent person to reevaluate potential noise doses.

c. Hazard Assessment

- (1) If consultation with a competent person indicates that noise doses could equal or exceed 100%, arrangements shall be made for a competent person to conduct noise monitoring to determine the noise dose.

⁵ Such a concern could be raised by any individual, e.g., a worker, a coworker, a supervisor, a Division Safety Representative, or a competent person.

⁶ For definitions of "Potential Noise Hazard," "Noise Hazard," and "Competent Person," see Section 7.

d. Control Methods

(1) Noise Doses that Equal or Exceed 100%

(a) Feasible⁷ engineering or administrative controls (such as noise-attenuating devices, worker relocation, and reduced exposure times) shall be implemented in an effort to reduce noise doses to less than 100%.

(b) If feasible engineering and administrative controls fail to reduce noise doses to less than 100%, HPDs identified by a competent person as providing sufficient noise attenuation shall be provided and used to reduce noise doses to less than 100%.

(3) Nuisance Noise

(a) If practicable, engineering and administrative controls should be implemented to reduce nuisance noise or exposure to nuisance noise.

(b) HPDs may be used to reduce exposure to nuisance noise provided that their use does not impede the ability of employees and associates to engage in necessary communications or to hear alarms or other notifications. Decisions to wear HPDs to reduce nuisance noise should be made on a case-by-case basis.

e. Use of HPDs

(1) HPDs other than ear muffs shall not be traded or shared in work areas in which unprotected employees and associates would receive noise doses that equal or exceed 100%.

(2) Ear muffs traded or shared in work areas in which unprotected employees and associates would receive noise doses that equal or exceed 100% shall be sanitized between uses.

(3) The use of audio headphones or ear buds in place of, or in conjunction with, HPDs is prohibited.⁸

⁷ OSHA currently considers feasible engineering and administrative controls to be those for which the costs of such controls are less than the cost of an effective Hearing Conservation Program.

⁸ OSHE may waive this requirement on a case-by-case basis, e.g., in the case of headphones which have been rated by ANSI for noise reduction and which have been determined by a competent person to provide sufficient noise attenuation.

f. Audiometric Testing

(1) All employees and associates required to wear HPDs to reduce noise doses to less than 100% shall be subject to the following audiometric testing requirements:

(a) Within 30 days of it being determined that an employee must wear HPDs, the employee must receive an audiogram administered by the Health Unit and to be used as the baseline against which subsequent audiograms are compared.

(b) Employees and associates required to wear HPDs must receive annual audiograms administered or arranged by the Health Unit.

(c) All baseline and repeat annual audiograms shall be preceded by at least 14 hours without exposure to workplace noise at levels above 80 dBA and should be preceded by at least 14 hours without exposure to non-workplace noise at levels above 80 dBA.⁹

(d) If an employee's annual audiogram shows a NIOSH significant threshold shift (NSTS) or an OSHA standard threshold shift (OSTS), the employee must receive a repeat audiogram administered by the Health Unit within 30 days.

g. Re-Review of Activity Hazard Reviews

(1) Upon determination by the Health Unit that an OSTS has occurred, the applicable activity hazard review shall be re-reviewed in accordance with the requirements of the Hazard Review suborder.

(2) As part of the re-review of the hazard review, a consultation shall be scheduled with a competent person to re-evaluate the noise exposures of affected employees and associates.

h. Training

(1) Training provided by OSHE on the NIST HPP shall be completed annually by employees and associates required to wear HPDs to reduce noise doses to less than 100%.

⁹When at least 14 hours without exposure to workplace noise cannot be achieved, HPDs identified previously by a competent person may be used as a substitute during that period for the requirement that baseline audiograms be preceded by at least 14 hours without exposure to workplace noise.

(2) Retraining provided by OSHE on the NIST HPP, including refitting of HPDs, should be completed by each employee who has been notified by the Health Unit that he or she has suffered a NSTS.

(3) Retraining provided by OSHE on the NIST HPP, including refitting of HPDs, shall be completed by each employee who has been notified by the Health Unit that he or she has suffered an OSTs.

(4) One-time-only training provided by OSHE on the NIST HPP shall be completed by Official First-Level Supervisors of employees and associates required to wear HPDs to reduce noise doses to less than 100%.

(5) One-time training provided by OSHE on the NIST HPP should be completed by employees and associates exposed to nuisance noise who elect, or who are mandated by their management, to wear HPDs.

(6) Training shall be recorded in accordance with the requirements of the NIST Safety Education and Training Program, and training records made available to affected employees and associates upon request.

i. Noise-Monitoring Records

(1) The results of hazard assessments, i.e., the results of consultations, including the results of sound-level-meter screening surveys, noise monitoring, identified engineering and administrative controls, and required HPDs, shall be noted, referenced, or included as part of the activity-hazard-review documentation.

(2) Noise-monitoring results requiring employees and associates to wear HPDs to reduce noise doses to less than 100% shall be provided to the Health Unit for inclusion in employee medical files.

j. Communication

(1) Hazard signage shall be posted at entrances to areas in which administrative controls or HPDs are required to reduce noise doses to less than 100%. Hazard signage shall clearly indicate the noise hazard and state the required administrative controls and HPDs. Appendix B provides an example of hazard signage meeting these requirements.

(2) Electronic or hard copies of this suborder and of [29 CFR 1910.95](#) shall be made available to affected employees and associates or their representatives.

k. Buy-Quiet Initiative

- (1) Manufacturers' noise specifications should be evaluated by a competent person prior to the purchase of equipment capable of producing noise hazards. If a quieter alternative is available, it should be considered; if not, the use of noise-attenuating devices should be considered.

7. DEFINITIONS

- a. Audibility Threshold – The sound intensity at a given frequency which is the minimum perceptible by a normal human ear under specified standard conditions.
- b. Audiogram – A chart, graph, or table resulting from an audiometric test showing an individual's hearing levels as a function of frequency.
- c. Audiologist – A professional specializing in the study and rehabilitation of hearing, and certified by the American Speech-Language-Hearing Association or licensed by a state board of examiners.
- d. Audiometric Test – A clinical evaluation of a person's hearing capacity using a calibrated, pure-tone audiometer and performed in accordance with OSHA 29 CFR 1910.95(g) and (h).
- e. Baseline Audiogram – An audiogram that is preceded by a 14-hour period of quiet and obtained from an audiometric examination administered before employment or within the first 30 days of employment.
- f. Certified Industrial Hygienist (CIH) – An individual who is board certified by the American Board of Industrial Hygiene and has met the minimum requirements for education, experience, and through examination has demonstrated a minimum level of knowledge in occupational health subject areas such as hearing protection.
- g. Certified Safety Professional (CSP) – An individual who is board certified by the Board of Certified Safety Professionals and has met the professional challenge of demonstrating competency through education, experience, and examination.
- h. Competent Person – A CIH or CSP in the NIST Office of Safety, Health and Environment (OSHE) or another NIST Organizational Unit (OU), a consultant CIH or CSP, or an individual directed by a CIH or CSP, who is capable of recognizing, controlling, and evaluating potential occupational hazards.

- i. dB – Decibel. See Sound Pressure Level.
- j. dBA – Unit representing the sound level measured in dB on the A-weighted scale of a sound-level meter. The A-weighted scale closely resembles how the human ear perceives common sounds.
- k. dB(C) – Unit representing the sound level measured in dB on the C-weighted scale of a sound-level meter. The C-weighted scale represents how the human ear perceives sound at high sound levels.
- l. Frequency – The number of cycles of a periodic motion per unit time. The SI unit of frequency is Hertz (Hz).
- m. Hearing Protection Device (HPD) - A type of personal protective equipment specifically designed to prevent hearing damage. Earplugs and earmuffs are the most common hearing protection devices.
- n. Hertz (Hz) – Unit of measurement of frequency, numerically equal to cycles/second (c/s).
- o. Intermittent Noise – Noise levels that are interrupted by intervals of relatively low sound levels.
- p. NIOSH Significant Threshold Shift (NSTS) – An increase in an individual’s audibility threshold value of 15 dB or more at any of the frequencies 500, 1000, 2000, 3000, 4000, or 6000 Hz, in either ear, from the baseline audiogram to the current audiogram.
- q. Noise Dosimeter – An instrument that integrates cumulative noise exposure over time and directly indicates noise dose. Noise dosimeters are used to conduct noise monitoring during a work day or monitoring period.
- r. Noise Hazard – Sound within the audible frequency range heard by the human ear (20 – 20,000 Hertz) at levels that, without controls, would result in employees and associates receiving noise doses that equal or exceed NIST noise dose limits (see Section 6a).
- s. Noise Monitoring – Process or method of measuring a person’s individual exposure to noise levels over a given time period.
- t. Nuisance Noise – Noise which would not result in employees and associates receiving noise doses that equal or exceed NIST noise dose limits (see Section 6a) but which is capable of causing discomfort.

- u. Octave Band Analyzer – A type of sound-level meter that can separate monitored noise levels into specific frequency bands.
- v. OSHA-Recordable Standard Threshold Shift – An OSTs in an individual with an overall hearing level of 25 dB or more above audiometric zero, averaged at the frequencies 2000, 3000, and 4000 Hz in the same ear as the OSTs, that has been determined by an audiologist or physician to be workplace-noise induced.
- w. OSHA Standard Threshold Shift (OSTS) – An increase of 10 dB or more in the average of an individual's audibility threshold values at the frequencies 2000, 3000, and 4000 Hz, in either ear, from the baseline audiogram to the current audiogram.
- x. Peak Noise Level – The highest instantaneous sound pressure level recorded during a measurement interval. Peak measurements are independent of noise dosimeter settings for response rate or weighting. According to [29 CFR 1910.95](#), unprotected employees and associates may not be exposed to peak noise levels greater than 140 dBC.
- y. Potential Noise Hazard – Sound within the audible frequency range heard by the human ear (20 – 20000 Hertz) that makes it difficult to have a conversation with someone three feet away, or has resulted in a complaint by one or more employees and associates, and to which there is a reasonable likelihood that employees and associates could be exposed.
- z. Sound-Level Meter – An instrument used to measure noise levels. A Type 1 sound-level meter is used for precision measurements in the field, and a Type 2 sound level-meter is used for general-purpose measurements.
- aa. Sound Pressure – The root-mean-square instantaneous sound pressure at a point during a given time interval.
- bb. Sound Pressure Level (dB) – Ten times the logarithm to the base ten of the ratio of the time-mean-square sound pressure, in a stated frequency band, to the square of the reference sound pressure in gases of 20 μ Pa.
- cc. Temporary Threshold Shift – A temporary shift in an ear's audibility threshold possibly caused by exposure to high-intensity acoustic stimuli. It also may be caused by the use of aspirin or other drugs.
- dd. Unprotected Employee – An employee not wearing hearing protection devices.

354 **8. ACRONYMS**

355 a. ACGIH – American Conference of Governmental Industrial Hygienists

357 b. ANSI – American National Standards Institute

359 c. CFR – Code of Federal Regulations

361 d. CIH – Certified Industrial Hygienist

363 e. CSP – Certified Safety Professional

365 f. HPD – Hearing Protection Device

367 g. HPP – Hearing Protection Program

369 h. NIOSH – National Institute of Occupational Safety and Health

371 i. NIST – National Institute of Standards and Technology

373 j. NSTS – NIOSH Significant Threshold Shift

375 k. OSHE – Office of Safety, Health, and Environment

377 l. OU – Organizational Unit

379 m. STS – Standard Threshold Shift

382 **9. ROLES AND RESPONSIBILITIES**

383 a. Employees and Associates Engaged in Activities that Could Result in Their Receiving Noise
384 Doses that Equal or Exceed 100%:

386 (1) If a concern arises regarding potential noise hazards in an already ongoing activity,
387 schedule a consultation with a competent person as soon as possible to determine if noise
388 doses could equal or exceed 100%;

390 (2) If the hazard review of a new activity identifies potential noise hazards, schedule a
391 consultation with a competent person to determine if noise doses could equal or exceed
392 100%;

- 394 (3) If the hazard review of a change in an existing activity identifies new noise hazards or
395 potential increases in previously identified noise hazards, schedule a consultation with a
396 competent person to reevaluate potential noise doses;
397
- 398 (4) Inform Official First-Level Supervisors of any consultations scheduled with competent
399 persons and of the results of those consultations;
400
- 401 (5) If consultation with a competent person indicates that noise dose could equal or exceed
402 100%, arrange for a competent person to conduct noise monitoring to determine the noise
403 dose;
404
- 405 (6) If the noise dose equals or exceeds 100%, implement feasible engineering or
406 administrative controls (such as noise-attenuating devices, worker relocation and reduced
407 exposure times) in an effort to reduce noise doses to less than 100%;
408
- 409 (7) If feasible engineering and administrative controls fail to reduce noise doses to less than
410 100%, use HPDs identified by a competent person to reduce noise doses to less than
411 100%; and
412
- 413 (8) Ensure that the results of hazard assessments, i.e., the results of consultations, including
414 the results of sound-level-meter screening surveys, noise monitoring, identified
415 engineering and administrative controls, and required HPDs, are noted, referenced, or
416 included as part of the activity-hazard-documentation.
417
- 418 b. Employees and Associates Required to Wear HPDs to Reduce Noise Doses to Less than
419 100% (in addition to the responsibilities of above):
420
- 421 (1) Use their HPDs in accordance with the requirements of the activity hazard review and
422 their training on HPD fit, use, and care;
423
- 424 (2) Participate in audiometric testing as specified in Section 9f;
425
- 426 (3) Complete the annual training provided by OSHE on the NIST HPP;
427
- 428 (4) Upon being notified by the Health Unit that they have suffered a NSTS, strongly consider
429 completing the retraining provided by OSHE on the NIST HPP, including refitting of
430 their HPDs, or complete this training if it is assigned to them by their official first-level
431 supervisors; and
432

(5) Upon being notified by the Health Unit that they have suffered an OSTs, complete the retraining provided by OSHE on the NIST HPP, including refitting of their HPDs.

c. Official First-Level Supervisors of Any of the Above Employees and Associates:

(1) Ensure that competent persons from outside of OSHE engaged by the OU to conduct hazard assessments and specify HPDs understand the responsibilities delineated below for competent persons;

(2) Provide the results of hazard assessments resulting in employees and associates being required to use HPDs to all such affected employees and associates, the OSHE Hearing Program Protection Manager, and the Health Unit for inclusion in employee medical files;

(3) Ensure that the results of hazard assessments are noted, referenced, or included as part of the activity-hazard-review documentation;

(4) Make electronic or hard copies of this suborder and of [29 CFR 1910.95](#) available to those employees and associates who are required to wear HPDs, or their representatives;

(5) Provide affected employees and associates with HPDs identified by competent persons as providing sufficient noise attenuation, at no cost to affected employees and associates;

(6) Provide affected employees and associates the opportunity to select HPDs from a variety of suitable HPDs;

(7) Assign training to affected employees and associates in accordance with the requirements in Section 6h;

(8) When employees and associates they supervise are required to wear HPDs, complete the one-time only training provided by OSHE on the NIST HPP;

(9) Make training records available to affected employees and associates upon request;

(10) Ensure that hazard signage meeting the requirements of Section 9j is posted at entrances to areas in which administrative controls or HPDs are required; And

(11) Upon being notified by the Health Unit that employees and associates they supervise have suffered workplace-noise-induced OSTs, ensure that all applicable activity hazard

reviews are re-reviewed in accordance with the requirements of the Hazard Review suborder, and, as part of the re-reviews, that consultations with competent persons are scheduled to re-evaluate the noise exposures of affected employees and associates.

d. Employees and Associates Exposed to Nuisance Noise:

- (1) Strongly consider completing the one-time-only training prescribed by OSHE on the NIST HPP.

e. OSHE Hearing Protection Program Manager:

- (1) Ensure that training provided by OSHE on the HPP is available and includes, at a minimum:

- (a) An overview of the NIST HPP;
- (b) Physical and psychological effects of noise and hearing loss;
- (c) Recognition of noise hazards;
- (d) Noise control principles:
 - i. Engineering controls;
 - ii. Administrative controls, including hazard signage; and
 - iii. HPDs, including selection, fit, use, and care; and

- (e) Overview of audiometric-testing requirements;

- (2) Ensure that training provided by OSHE on the HPP is documented in NIST's electronic safety training application;

- (3) Ensure that non-web-based training provided by OSHE on the HPP and completed by affected employees and associates is recorded in NIST's electronic safety training application;

- (4) Ensure that all OSHA-recordable OSTs are recorded on the OSHA 300 log maintained by OSHE in accordance with the requirements of [29 CFR 1904.10](#), Recording of Cases Involving Occupational Hearing Loss; and

(5) Assist NIST staff in the development of signage that complies with the requirements of this suborder and the NIST Hazard Signage Program.

f. Competent Persons:

(1) Consult with potentially affected employees and associates to determine if noise doses could equal or exceed 100%;

(2) When it has been determined that noise doses could equal or exceed 100%, conduct noise monitoring, document the results in writing, and provide those results to the employee who scheduled the assessment and his or her Official First-Level Supervisor;

(3) When conducting noise monitoring, inform affected employees and associates in areas being monitored, along with any designated employee representatives, of the purpose of the noise monitoring and provide them with the opportunity to observe noise-monitoring activities;

(4) When employees and associates are required to wear HPDs to reduce noise doses to less than 100%, specify the necessary protection in accordance with [29 CFR 1910.95](#), [Appendix B](#): "Methods for Estimating the Adequacy of Hearing Protection Attenuation;

(5) Recommend a variety of suitable HPDs for selection and proper fit; and

(6) If noise monitoring identifies a potential noise hazard or a potential increase in a previously identified noise hazard, work with affected employees and associates to ensure that noise doses do not equal or exceed 100%;

(7) Ensure that:

(a) Noise screening and octave-band analysis is conducted using ANSI Type 1 or Type 2 sound-level meters;

(b) Noise monitoring is conducted using ANSI Type 2 noise dosimeters;

(c) Noise dosimeters used for noise monitoring integrate all sound levels between 80 dBA and 130 dBA and measure peak sound levels up to and including 140 dB; and

(d) Sound-level meters and noise dosimeters are calibrated at least annually and according to manufacturers' specifications; and

(8) Re-evaluate the noise exposures of employees and associates who have suffered workplace-noise-induced OSTs.

g. Each Health Unit:

(1) Maintain an audiometric testing program in accordance with 29 CFR 1910.95(g), Audiometric Testing Program;¹⁰

(a) Notify employees and associates that during the 14-hour period immediately preceding a baseline or repeat annual audiometric examination, they must avoid exposure to workplace noise at levels above 80 dBA and should avoid exposure to non-workplace noise at levels above 80 dBA;

(2) Conduct audiometric tests in accordance with 29 CFR 1910.95(h), Audiometric Test Requirements;

(3) Determine whether NSTs and OSTs have occurred, and upon determining that they have, notify affected employees and associates, affected employees' and associates' Official First-Level Supervisors, OU Safety Coordinators, and the OSHE Hearing Protection Program Manager in writing within 21 days;

(4) Upon determining that OSTs have occurred, arrange for audiological evaluations as necessary to assist in determining whether the OSTs are workplace-noise induced;

(5) Upon determining that OSTs are workplace-noise induced, notify affected employees and associates, affected employees and associates' Official First-Level Supervisors, OU Safety Coordinators, and the OSHE Hearing Protection Program Manager; and

(6) Maintain audiometric test records in accordance with 29 CFR 1910.95(m), Recordkeeping.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

¹⁰ NIST does not use age correction to attempt to differentiate between hearing losses caused by age-related factors and those caused by noise exposures.

589 **11. DIRECTIVE OWNER**

590 Chief Safety Officer

591

592

593 **12. APPENDICES**

594 a. Appendix A. Revision History

595 b. Appendix B. Hazard Signage

596

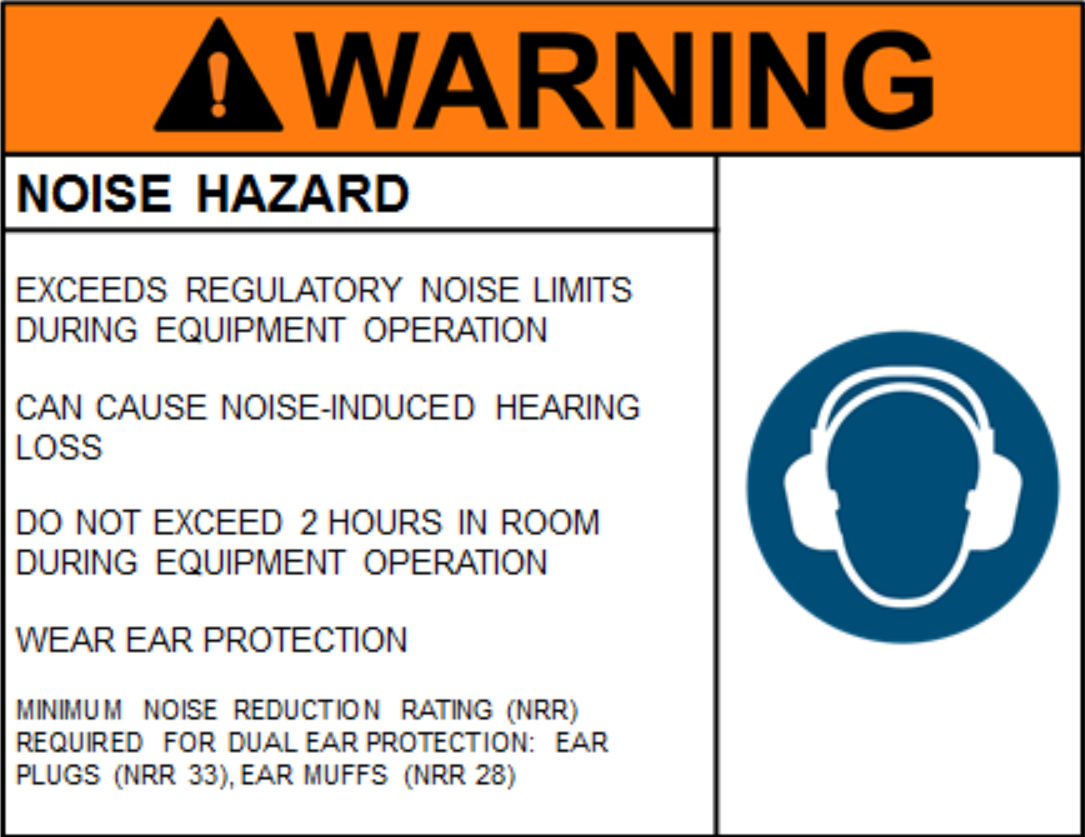
597
598

Appendix A. Revision History

Revision	Date	Responsible Person	Description of Change
0	03/20/2014	Amber Carlberg	None – Initial suborder approval
1	02/06/2015	Richard Kayser	<ol style="list-style-type: none">1. Addition of Revision History in Appendices.2. Revisions throughout to include NIST associates.3. Addition of NIOSH Significant Threshold Shift.4. Inclusion of statement that it is NIST policy not to use age-correction factors.5. Addition of audiological evaluations to assist in making determinations of work-relatedness.

599

APPENDIX B: HAZARD SIGNAGE



3 Control of Hazardous Energy 4 (Lockout/Tagout)

5
6 NIST S 7101.56

7 Document Approval Date: 11/05/2015

8 Effective Date:¹ 11/05/2015
9
10

11 1. PURPOSE

12 This suborder establishes the safety requirements necessary to protect NIST employees and
13 associates from exposure to hazardous energy during the servicing or maintenance of machines
14 or equipment (hereafter referred to as “equipment”), and the organizational roles and
15 responsibilities for ensuring that those requirements are met.
16
17

18 2. BACKGROUND

19 a. NIST must meet or exceed the requirements established by OSHA in [29 Code of Federal](#)
20 [Regulations \(CFR\) 1910.147](#), The Control of Hazardous Energy. Implementation of this
21 suborder through the requirements in Section 6 and the roles and responsibilities in Section 9
22 meets those requirements.
23

24 b. This suborder supersedes NIST Health and Safety Instruction (HSI) 21, Control of
25 Hazardous Energy (Lockout/Tagout), June 1994.
26
27

28 3. APPLICABILITY

29 a. The provisions of this suborder apply to equipment servicing and maintenance activities,
30 conducted by NIST employees, associates, or contractors, that could harm NIST workers if
31 the equipment being serviced or maintained were to unexpectedly energize, start up, or
32 release stored energy.
33

34 (1) When servicing or maintenance activities are conducted exclusively by outside
35 contractors, OUs need only follow Section 6g and meet the Affected-Worker training
36 requirements in Section 6j(1)(b)i.

¹ For revision history, see Appendix A.

b. Applicability to Normal Production Operations.

(1) The provisions of this suborder apply to servicing and maintenance that takes place during normal production operations only when:

(a) A NIST employee or associate is required to remove or bypass a guard or other safety device; or

(b) A NIST employee or associate is required to place any part of his/her body into an area on a piece of equipment where work is actually performed or where an associated danger zone exists during an equipment operating cycle.

(2) The provisions of this suborder do not apply to minor tool changes and adjustments and other minor servicing activities that take place during normal production operations if these activities are routine, repetitive, and integral to the use of the equipment for production, provided that the work is performed using alternative measures, such as machine guarding, that provide effective protection.

c. For exposure² to electrical hazards (e.g. shock, arc flash) from work on, near, or with conductors or equipment in electric-utilization installations, the provisions of this suborder are part of a larger set of requirements defined fully in NIST Notice 7101.64, Electrical Safety.

d. Exclusions. The provisions of this suborder do NOT apply to:

(1) Work on cord- and plug-connected electrical equipment meets ALL of the following conditions:

(a) The equipment has a single energy source;

(b) All hazardous energy to which workers could be exposed can be controlled by unplugging the equipment; and

(c) The plug is under exclusive control of the worker servicing or maintaining the equipment.

² Exposed (as applied to energized electrical conductors or circuit parts) – Capable of being inadvertently touched or approached nearer than a safe distance by a person. It is applied to electrical conductors or circuit parts that are not suitably guarded, isolated, or insulated.

(1) Hot-tap operations involving transmission and distribution systems for substances such as gas, steam, water, or petroleum products are performed on pressurized pipelines, provided that it can be demonstrated that:

(a) Continuity of service is essential;

(b) Shutdown of the system is impractical;

(c) Special equipment (e.g., bolted blinds and blank flanges) is used which will provide proven effective protection for NIST employees and associates; and

(d) Documented procedures are followed.

4. REFERENCES

- a. [29 CFR 1910.147](#), The Control of Hazardous Energy (lockout/tagout).
- b. [29 CFR 1910.333](#), Selection and use of work practices.
- c. ANSI Z535.5, Safety Tags and Barricade Tapes (for Temporary Hazards) (most recent version).
- d. [NIST O 710](#), Occupational Safety and Health Management System.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews
- b. NIST S 7101.63: Electrical Safety

6. REQUIREMENTS

- a. General Requirements

(1) OUs shall establish energy-control procedures, worker training, and annual inspections prior to conducting servicing or maintenance on equipment where the unexpected energizing, startup, or release of stored energy could occur and cause injury.

113 (2) Tagout without Lockout
114

115 (a) If an energy-isolating device is not capable of being locked out, a tagout system shall
116 be used.

117
118 (b) If an energy-isolating device is capable of being locked out, lockout shall be used
119 unless it can be demonstrated that the utilization of a tagout system will provide
120 employees and associates with full protection, which requires that ALL of the
121 following be met:

122
123 i. The tagout device shall be attached at the same location that the lockout device
124 would have been attached.

125
126 ii. Full compliance with all tagout-related provisions of this suborder shall be
127 demonstrated.

128
129 iii. Such additional elements as are necessary to provide the equivalent safety
130 available from the use of a lockout device shall be demonstrated. Additional
131 means to be considered shall include the implementation of additional safety
132 measures such as removal of an isolating circuit element, blocking of a
133 controlling switch, opening of an extra disconnecting device, or removal of a
134 valve handle to reduce the likelihood of inadvertent energization. They could also
135 include a rigorous training program and demonstrated compliance over time.

136
137 (c) Whenever replacement or major repair, renovation, or modification of equipment is
138 performed, and whenever new equipment is installed, energy-isolating devices for
139 such equipment shall be designed to accept a lockout device whenever the unexpected
140 energization or startup of the equipment, or release of stored energy, could cause
141 injury to workers.

142
143 b. Requirement for Written LOTO Procedures
144

145 (1) Written LOTO procedures are required unless ALL of the following circumstances
146 pertain:

147
148 (a) The equipment has no potential for stored or residual energy or re-accumulation of
149 stored energy after shut down which could endanger workers;

150
151 (b) The equipment has a single energy source which can be readily identified and
152 isolated;

- 153 (c) The isolation and locking out of that energy source will completely de-energize and
154 deactivate the equipment;
155
- 156 (d) The equipment is isolated from that energy source and locked out during servicing or
157 maintenance;
158
- 159 (e) A single lockout device will achieve a locked-out condition;
160
- 161 (f) The lockout device is under the exclusive control of the Authorized Worker
162 performing the servicing or maintenance;
163
- 164 (g) The servicing or maintenance does not create hazards for Other Workers; and
165
- 166 (h) The OU, in utilizing this exception, has had no accidents involving the unexpected
167 activation or re-energization of the equipment during servicing or maintenance.
168
- 169 (2) If a written procedure is required, the Authorized Worker shall:
170
- 171 (a) Use NIST's online energy-control procedure application to develop an equipment-
172 specific LOTO procedure; or
173
- 174 (b) If not using NIST's online energy-control procedure application, ensure that the
175 procedure clearly and specifically outlines the scope, purpose, authorization, rules,
176 and techniques to be utilized for the control of hazardous energy, and the means to
177 enforce compliance, including, but not limited to, the following:
178
- 179 i. A specific statement of the intended use of the procedure;
180
- 181 ii. Specific procedural steps for shutting down, isolating, blocking, and securing the
182 equipment to control hazardous energy;
183
- 184 iii. Specific procedural steps for the placement, removal, and transfer of LOTO
185 devices and the responsibility for them; and
186
- 187 iv. Specific requirements for testing the equipment to determine and verify the
188 effectiveness of LOTO devices and other energy-control measures.
189
190
191
192

c. Conduct of LOTO

LOTO shall be performed only by trained Authorized Workers in the following sequence:

- (1) Notifications shall be initiated prior to LOTO to ensure area supervisors and affected personnel are aware of the energy source being locked out or controlled. This notification should also include the anticipated duration of the shutdown. Authorized Workers will also advise on any support equipment that may be impacted, additional safety precautions being taken, and the type of control device(s) being used.
- (2) Preparations for the shutdown shall begin after all notifications have been made. Authorized Workers must be fully aware of the type and magnitude of the energy, associated hazards, and control methods of the energy involved. Authorized Workers shall refer to owner/service manuals of the equipment they are working on to ensure they are fully aware of any and all associated hazards.
- (3) In performing the shutdown, Authorized Workers shall first advise Affected Workers that shutdown is taking place. They shall then locate the energy source(s) (always looking for hidden energy sources) and follow the procedures established to shut down the equipment as prescribed. An orderly shutdown must be utilized to avoid any additional or increased hazard(s) to workers as a result of the equipment stoppage.
- (4) All energy-isolating devices that are needed to control the energy to the equipment shall be physically located and operated by an Authorized Worker in such a manner as to isolate the equipment from the energy source(s).
- (5) LOTO devices shall be affixed to energy-isolating devices by Authorized Workers.
 - (a) Lockout devices, where used, shall be affixed in a manner that will hold the energy-isolating devices in a "safe" or "off" position.
 - (b) Tagout devices, where used in accordance with this suborder, shall be affixed in such a manner as will clearly indicate that the operation or movement of energy-isolating devices from the "safe" or "off" position is prohibited. Where tagout devices are used with energy-isolating devices designed with the capability of being locked, the tag attachment shall be fastened at the same point at which the lock would have been attached. Where a tag cannot be affixed directly to the energy-isolating device, the tag shall be located as close as safely possible to the device, in a position that will be immediately obvious to anyone attempting to operate the device.

(6) After LOTO devices have been applied to energy-isolating devices, all potentially hazardous stored or residual energy shall be relieved, disconnected, restrained, or otherwise rendered safe. If there is a possibility of re-accumulation of stored energy to a hazardous level, verification of isolation shall be continued until the servicing or maintenance is completed, or until the possibility of such accumulation no longer exists.

(7) Prior to starting work on equipment that has been locked or tagged out, the Authorized Worker shall verify that isolation and de-energization of the equipment have been accomplished.

(8) Before LOTO devices are removed and energy is restored to the equipment, actions shall be taken by the Authorized Worker(s) to ensure that:

(a) The work area is inspected to ensure that any nonessential items have been removed and that the equipment components (e.g., guards) are operationally intact; and

(b) The work area is checked to ensure that all workers have been safely positioned or removed.

(c) After LOTO devices have been removed by the Authorized Worker(s) who applied them but before energy is restored to the equipment, Affected Workers shall be notified of the removal of the LOTO devices.

i. When the Authorized Worker who applied a LOTO device is unavailable to remove it, that device may be removed under the procedures outlined in Section 6h.

d. Temporary Removal of LOTO Devices

In situations in which LOTO devices must be temporarily removed from the energy-isolating device and the equipment energized to test or position it or a component thereof, the following sequence of actions shall be followed:

(1) Clear the equipment of tools and materials;

(2) Remove workers from the equipment area;

(3) Remove the LOTO devices;

(4) Energize and proceed with testing or positioning; and

(5) De-energize all systems and reapply energy-control measures in accordance with Section 6c of this suborder to continue the servicing and/or maintenance.

e. Group LOTO Procedure

When multiple Authorized Workers (including servicing contractors) perform service or maintenance on the same piece of equipment, a supervisor may determine that a group LOTO procedure is appropriate.

(1) When servicing or maintenance is performed by a crew, craft, department, or other group, that entity shall utilize a procedure that affords the workers a level of protection equivalent to the implementation of a personal LOTO device.

(2) The supervisor shall convene a meeting of all group members covered under the procedure.

(3) The supervisor shall describe the tasks to be performed and document those tasks in a written energy-control procedure.

(4) The supervisor may delegate an Authorized Worker the primary responsibility for a specified group working under the protection of the group LOTO procedure. Supervisory responsibility is then vested in the Designated Lead Authorized Worker for the specific workers working under the protection of the group LOTO devices.

(5) Each member of the specified group shall be trained and Authorized as described in this suborder's training requirements.

(6) The Designated Lead Authorized Worker shall ensure that each step of the written LOTO procedure has been completed and shall ascertain the exposure status of individual group members with regard to the lockout or tagout of the equipment.

(7) Each Authorized Worker performing work on the equipment shall ensure every step of the written procedure has been completed prior to placing their personal LOTO device on the group LOTO device, group lockbox, or comparable mechanism when he/she begins work.

(8) When the work has been completed, and after each worker has removed his/her respective lock or tag from the group LOTO device, the Designated Lead Authorized Worker shall remove his/her LOTO lock or tag from the group LOTO device and return the equipment to service as described in the procedure.

f. LOTO Procedures for Shift Changes

Specific procedures shall be utilized during shift or personnel changes to ensure the continuity of LOTO protection, including provision for the orderly transfer of LOTO device protection between departing and oncoming workers, to minimize exposure to hazards from the unexpected energization or start-up of the equipment, or the release of stored energy.

(1) If equipment will remain de-energized after the end of a shift and work on it is to continue on the oncoming shift, the following criteria must be met:

(a) A justifiable and verifiable need must be identified;

(b) Formal approval from line management must be obtained; and

(c) A group LOTO device must be utilized.

(2) If these criteria have been met, an orderly transfer of LOTO devices between Authorized Workers must be performed in accordance with the following procedure:

(a) The Authorized Workers from both shifts must be present at the LOTO device;

(b) The departing Authorized Worker must inform the oncoming Authorized Worker of any potential hazards;

(c) The oncoming Authorized Worker must place his/her lock and/or tag onto the group LOTO device, and the departing Authorized Worker must remove his/her lock and/or tag from the group LOTO device; and

(d) Before work begins, the oncoming Authorized Worker(s) shall verify isolation and de-energization of the equipment that has been locked or tagged out prior to restarting work.

(3) When there is a gap between shifts and a meeting between departing and incoming Authorized Workers does not occur, the departing Authorized Workers' LOTO devices shall remain in place. The oncoming Authorized Worker working on that equipment shall add his/her LOTO lock and/or tag to the group LOTO device and work following the requirements of this document. This worker shall remove his/her LOTO lock and/or tag when finished working on the equipment.

g. LOTO Procedures for Working with Contractors

(1) Contractors shall not be permitted to commence servicing or maintenance work on NIST equipment when LOTO is required until:

(a) They have been provided with a copy of this suborder by the controlling NIST organization;

(b) They have exchanged LOTO programs with the controlling NIST organization;

(c) The exchange of LOTO programs has been documented using the exchange-of-LOTO-programs form provided by OSHE; and

(d) Information concerning contractor LOTO procedures has been communicated to NIST Affected Workers.

h. LOTO Device Emergency Removal

WARNING: This is considered to be an emergency procedure only to be undertaken in extreme circumstances with a supervisor's approval and using extreme care.

(1) When an Authorized Worker who has applied a LOTO device is not available to remove it, his/her immediate supervisory chain may authorize its removal in accordance with this emergency removal procedure. If the Authorized Worker's immediate supervisor is not available, the emergency removal may be performed by one level of management above the Authorized Worker's immediate supervisor or by a delegated individual with documented authorization from the immediate supervisor.

(2) The following steps must be performed and documented using the Emergency LOTO Lock Removal form provided by OSHE.

(a) The supervisor must verify the Authorized Worker is not at the NIST facility. The supervisor must make every reasonable effort to contact the Authorized Worker. This may include a telephone call to the worker's home or other location. These efforts must be documented (e.g., email, registered letter, voicemail, or telephone verbal assurance, etc.) by the supervisor.

(b) If the Authorized Worker is contacted, the supervisor must inform the worker that his/her LOTO device is being removed.

(c) The supervisor must verify that it is safe to remove the LOTO device.

(d) The supervisor may then authorize another Authorized Worker to remove the LOTO device.

(e) The supervisor must ensure that before the LOTO device owner returns to work, he/she is presented with the removed device and is informed of the reasons for the emergency removal.

(f) The emergency procedure form must be signed by the supervisor and the Authorized Worker who removed the lock and be retained in the OU's LOTO records.

i. Locks, Tags, and Devices

Locks, tags, chains, wedges, key blocks, adapter pins, self-locking fasteners, or other hardware shall be provided by the OU for isolating, securing, or blocking of equipment from hazardous-energy sources.

(1) General lockout device and tag requirements include:

(a) Locks and tags must be singularly identifiable;

(b) Locks and tags must be the only devices used for controlling hazardous energy during LOTO activities and not be used for any other purpose (e.g. restricting access);

(c) Locks and tags must be durable enough to withstand wet, damp, and corrosive environments while they are in use on equipment, including ensuring the print on the tag does not become illegible;

(d) Locks must be substantial enough to prevent removal without the use of excessive force or unusual techniques such as using bolt cutters or other metal cutting tools.

(e) Tags must be substantial enough to prevent inadvertent or accidental removal, which means that they must have an attachment means of a non-reusable type, be attachable by hand, be self-locking, and be non-releasable with a minimum unlocking strength of no less than 50 pounds, i.e., they must have characteristics similar to those of a one-piece all-environment-tolerant nylon cable tie; and

(f) Locks and tags shall be standardized in at least one of the following criteria: color, shape, or size; additionally, in the case of tagout devices, print and format shall be standardized.

432 (2) NIST's LOTO device requirements are as follows:

433
434 (a) Personal locks shall have red bodies and singular keys.

435
436 i. Authorized Workers with multiple personal locks may have them keyed alike.

437
438 ii. Personal locks must contain the identity of the Authorized Worker who applies
439 them.

440
441 iii. Supervisors of Authorized Workers may maintain copies of the keys to the
442 Authorized Workers' personal locks to be used for emergency device removal
443 only.

444
445 (b) Equipment locks shall have red bodies and may be keyed alike.

446
447 (c) Lockout tags must meet the following ANSI Z535.5 criteria:

448
449 i. Danger tags shall have the word "Danger" in safety white letters on a rectangular
450 safety red background;

451
452 ii. Danger tags will be on a safety white stock;

453
454 iii. Danger tags must contain the action statement, "Do Not Operate," and, at a
455 minimum, the Authorized Worker's name and phone number; pictures and other
456 information may also be applied to the tags;

457
458 iv. Tag message lettering should be typed; if printed messages are applied, they must
459 be legibly printed; and

460
461 v. Backs of tags may be used to give additional operating instructions, emergency
462 procedures, emergency telephone numbers, or to reinforce the critical role that the
463 LOTO tag holds; the back side of the tag should refer to the front side of the tag
464 and vice versa.

465
466 (3) The following considerations apply to personal versus equipment lockout devices:

467
468 (a) Personal lockout devices are to be used by Authorized Workers and must be placed
469 along with a LOTO tag at each energy-isolation point as directed by the specific
470 LOTO procedure; and
471

(b) Equipment locks are to be used by Authorized Workers when equipment has multiple energy-isolation points requiring the use of multiple LOTO locks. The keys for those locks are placed inside a group lock box that is secured using a personal lock and tag.

j. Training

(1) Training of Authorized, Affected , and Other Workers and their Official First-Level Supervisors

(a) Authorized Workers shall complete:

- i. The training provided by OSHE on the Control of Hazardous Energy (LOTO) program;
- ii. The activity-specific training required by hazard reviews applicable to the work to be conducted, including
 - (i) The recognition of applicable hazardous-energy sources;
 - (ii) The types and magnitudes of those hazardous-energy sources; and
 - (iii) The methods and means necessary for energy isolation and control, and where tagout only is used, review of the following key points:
 - Tags are essentially warning devices and do not provide physical restraint like a lock.
 - When a tag is attached to an energy-isolating device, it is not to be removed without authorization from the Authorized Worker identified on the tag, and it is never to be bypassed, ignored, or otherwise defeated.
 - Tags shall be legible and understandable by all workers.
 - Tags and their means of attachment shall be made of materials that will withstand environmental conditions encountered while on equipment.
 - Tags may evoke a false sense of security and their meaning needs to be understood as part of the overall energy-control program.

- Tags shall be securely attached to energy-isolating devices so they cannot be inadvertently or accidentally detached during use.
- (b) Affected Workers shall complete activity-specific training on the purpose and use of the energy-control procedures applicable to their assigned duties and work locations and of the prohibition of attempts to re-start or re-energize equipment that is locked or tagged out.
- i. When only contractors perform LOTO, Affected Workers shall understand and comply with the restrictions and prohibitions of the outside employer's energy control program.
- (c) The activity-specific training for Authorized and Affected Workers shall be provided by Authorized Workers who have successfully completed training on the Control of Hazardous Energy (LOTO) program and who are familiar with the applicable energy sources and the methods and means of energy isolation and control.
- (d) Official First-Level Supervisors of Authorized Workers shall complete the training provided by OSHE on the Control of Hazardous Energy (LOTO) program.
- (e) Other Workers shall complete training provided by OSHE on the general purpose and use of energy-control procedures and of the prohibition of attempts to re-start or re-energize equipment that is locked or tagged out.³
- (2) Retraining of Authorized and Affected Workers
- (a) Authorized and Affected Workers shall complete activity-specific retraining whenever:⁴
- i. A change in their job assignment requires Authorized and Affected Workers to service and maintain or operate additional equipment or introduces them to new energy sources;
- ii. A change in equipment or its operation presents a new hazard;
- iii. A change in LOTO procedures is introduced;

³ This training is part of NIST General Safety Training, which is provided automatically by the NIST electronic safety-training application to all employees and associates entering on duty.

⁴ The requirements in Sections 6j(2)i-iii coincide with requirements in the Hazard Review suborder (a) to conduct hazard reviews when changes to existing activities introduce new or increase existing hazards, and (b) for the authorization of workers.

- iv. A LOTO annual inspection points to a systemic deficiency warranting retraining;
or
- v. A LOTO annual inspection, observation, or other condition reveals deviations from LOTO procedures or a worker is found to lack knowledge of those procedures.
- (3) Documentation and Records
- (a) Training shall be documented and recorded in accordance with the requirements, roles, and responsibilities in the Safety Education and Training suborder.
- k. LOTO Annual Inspections
- (1) Annual Inspection of LOTO Procedures.
- (a) Each energy-control procedure, whether written and unwritten, shall be separately inspected annually to ensure that the energy-control procedure is adequate and is being properly implemented by Authorized Workers.
- (b) At a minimum, these inspections shall include a demonstration of the procedures by Authorized Workers while servicing and/or maintaining equipment.
- (c) The inspector, who must be an Authorized Worker other than the one(s) utilizing the energy-control procedure being inspected, shall observe the implementation of the energy-control procedure for the servicing and/or maintenance being evaluated and talk with employees and associates implementing the procedure to determine that all the requirements of this suborder are understood and being followed.
- i. The Authorized Worker performing the inspection may be someone who previously has or currently implements the energy-control procedure being inspected, as long as he/she is not implementing any part of the energy-control procedure while it is being inspected.
- (d) The inspector must be able to determine whether:
- i. The steps in the energy-control procedure are being followed;
- ii. The workers involved know their responsibilities under the procedure; and

iii. The procedure is adequate to provide the necessary protection, and, if inadequate, what modifications are needed.

(e) Procedures may be reviewed together during one inspection as long as they involve the same or similar types of energy-control methods.

i. If procedures are grouped together for annual inspection, it is recommended that one or more of the individual procedures (from the same group or from similar procedures from the previous year) be reviewed on its own so that over time each procedure is reviewed individually.

(2) Inspection Records

(a) Annual inspections shall be recorded using the LOTO inspection form provided by OSHE and maintained by the OU until the completion of the next annual inspection. If inspections reveal inadequate or improper LOTO procedures, the hazard or discrepancy must be mitigated immediately and Authorized and Affected Workers must be retrained as indicated in Section 6j.

7. DEFINITIONS

- a. Affected Worker – Any worker who uses equipment subject to being serviced or maintained under LOTO, or whose job requires him or her to work in an area in which such servicing or maintenance is being performed.
- b. Authorized Worker – A person who has completed the required hazardous-energy-control training (general and procedure-specific) and is authorized by their Division Chief or designee to lock and tag out the energy-control points in specific equipment or apparatus in order to perform service or maintenance. A person must be an Authorized Worker to apply a lock or tag to control hazardous energy.
- c. Capable of Being Locked Out – An energy-isolating device is considered capable of being locked out if it has a hasp or other means to attach a lock, has a locking mechanism built into it, or can be locked without dismantling, rebuilding, or replacing the energy-isolating device or permanently altering its energy-control capability.
- d. Energized – Connected to an energy source or containing stored energy.
- e. Energy-Isolating Device – A mechanical device that physically prevents the transmission or release of energy, including but not limited to the following: a manually operated electrical-

circuit breaker; a disconnect switch; a manually-operated switch by which the conductors of a circuit can be disconnected from all ungrounded supply conductors and, in addition, no pole can be operated independently; a line valve; a block; and any similar device used to block or isolate energy. Push buttons, selector switches, and other control-circuit-type devices are not energy-isolating devices.

- f. Energy-Isolation Point – A location at which the flow or release of hazardous energy can be prevented when a mechanism such as a valve, breaker, switch, blank off, or block-out is placed in the “OFF” position. Control circuits such as computer-control circuitry and software are not energy-isolation points.
- g. Equipment Locks – Locks used to perform LOTO on equipment with multiple energy-isolation points.
- h. Exclusive Control – A condition in which a worker has taken actions or is continuously in a position to prevent (exclude) other individuals from re-energizing or starting equipment while it is being serviced or maintained.
- i. Group Lock Box – A key box containing the key(s) used to lock out equipment being serviced by multiple Authorized Workers. Each Authorized Worker involved in the servicing places his/her personal locks on the group lock box. The keys to the equipment cannot be accessed until all Authorized Workers remove their locks.
- j. Group LOTO – A procedure to coordinate service or maintenance work by several Authorized Workers on locked/tagged out equipment. More than one Authorized Worker may need access to the locked/tagged out equipment because it has multiple energy sources, requires multiple LOTO procedures, or the work to be performed extends across shifts.
- k. Hazardous Energy – Energy capable of causing personal harm or property damage if it is not controlled. Types of hazardous energy include, but are not limited to, electrical, mechanical, rotational, gravitational, chemical, radioactive, hydraulic, pneumatic, and thermal.
- l. Hazardous-Energy Control – The process of systematically implementing engineering and administrative means to prevent hazardous energy from flowing to a person.
- m. Hazardous-Energy-Control Procedure – An equipment-specific procedure Authorized Workers must follow to safely control hazardous energy during servicing or maintaining of the equipment.

- n. Hazardous-Energy Source – Equipment, machine, apparatus, process piping, and so on, which is a source of hazardous energy.
- o. Hot Tap – A procedure used in servicing and/or maintenance that involves welding on a piece of equipment (pipelines, vessels, or tanks) under pressure, in order to install connections or appurtenances. Hot taps are commonly used to replace or add sections of pipeline without the interruption of service for air, gas, water, steam, and petrochemical distribution systems.
- p. Lockout – The placement of a lockout device on an energy-isolating device, in accordance with an established procedure, to ensure the energy-isolating device and the equipment being controlled cannot be operated until the lockout device is removed.
- q. Lockout Device – Any device that uses a positive means such as a lock, blank flanges, and bolted slip blinds to hold an energy-isolating device in a safe position to prevent equipment from unexpectedly energizing.
- r. Normal Operations – The utilization of equipment to perform intended functions.
- s. Other Worker – A worker with duties that are or may be in an area where energy-control procedures may be utilized.
- t. Personal Lock – A singularly keyed lock issued to an Authorized Worker used exclusively for the control of hazardous energy.
- u. Servicing and/or Maintenance – Workplace activities such as constructing, installing, setting up, adjusting, inspecting, and modifying equipment that could expose workers to the unexpected release of hazardous energy. Maintenance activities may also include lubrication, cleaning, or unjamming equipment, and making adjustments or tool changes.
- v. Setting up – Any work performed to prepare equipment to perform its normal operation.
- w. Stored Energy – Energy located within any device after equipment is shut down. This includes, but is not limited to, capacitors, tanks, pipes, springs, and flywheels.
- x. Tagout – The placement of a tagout device on an energy-isolating device, in accordance with an established procedure, to indicate that the energy-isolating device and the equipment being controlled shall not be operated until the tagout device is removed.

- y. Tagout Device – A prominent warning device, such as a tag and a means of attachment that can be securely fastened to an energy-isolating device in accordance with an established procedure, to indicate that the energy-isolating device and the equipment being controlled may not be operated until the tagout device is removed.

8. ACRONYMS

- a. LOTO – Lockout/Tagout
- b. OSH – Occupational Safety and Health
- c. OSHE – Office of Safety, Health, and Environment
- d. OU – Organizational Unit

9. ROLES AND RESPONSIBILITIES

- a. OUs:
- (1) Ensure that the requirements in Section 6 are met.
- b. Chief Safety Officer:
- (1) Ensure that the training specified in Sections 6j(1)(c) for Other Workers is included in NIST General Safety Training.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

A. Revision History

743
744

Appendix A. Revision History

Revision No.	Approval Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	03/20/14	06/25/14	04/01/15	None – Initial document
1	11/05/15	11/05/15	11/05/15	<ul style="list-style-type: none">• Made suborder applicable to “associates”.• Added new Section 3c(1) to clarify the relationship between this suborder and NIST N 7101.64, Electrical Safety; added “to which workers could be exposed” to Section 3c(2)(b).

745

Permit-Required Confined Spaces

NIST S 7101.57

Document Approval Date: 05/16/2014

Effective Date: 04/01/2015

1. PURPOSE

The purpose of this suborder is to establish the safety requirements for identifying, evaluating, and entering permit-required confined spaces (hereafter referred to as “permit spaces”) and the organizational roles and responsibilities for ensuring that those requirements are met.

2. BACKGROUND

- a. NIST must meet or exceed the requirements established by the Occupational Safety and Health Administration (OSHA) in 29 Code of Federal Regulations (CFR) 1910.146, Permit-Required Confined Spaces. Implementation of this suborder through the requirements in Section 6 and roles and responsibilities in Section 9 fulfills those requirements.
- b. This suborder, all supporting suborder-specific directives, including procedures, guidance, and notices, and all required deployment tools, including training, forms, instructions, and information technology applications, constitute the written permit-required confined-space program required by 29 CFR 1910.146(c)(4).
- c. This suborder supersedes NIST Health and Safety Instruction (HSI) 9, Work in Confined Spaces, November 1994.

3. APPLICABILITY

- a. The provisions of this suborder apply to NIST employees and to contractors who are to enter or potentially be exposed to permit spaces.

4. REFERENCES

- a. [29 CFR Part 1910.146](#), Permit-Required Confined Spaces; and
- b. [29 CFR 1910.147](#), The Control of Hazardous Energy (Lockout/Tagout).

40 **5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS**

41 a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;

43 b. NIST S 7101.21: Personal Protective Equipment;

45 c. NIST S 7101.56: Control Of Hazardous Energy (LOTO);

47 d. NIST S 7101.59: Chemical Hazard Communication; and

49 e. NIST S 7101.22: Hazard Signage.

52 **6. REQUIREMENTS¹**

53 a. Hazard Identification

55 (1) Determine if confined spaces are present in OU work areas.

57 b. Hazard Assessment

59 (1) As part of the hazard review process, assess the hazards in any confined spaces identified
60 to determine if those spaces meet the definition of a permit space.

62 (2) If an identified confined space meets the definition of a permit space, classify that space
63 as a permit space; otherwise classify it as a non-permit space.

65 (3) For spaces classified as permit spaces, post danger signs or use other equally effective
66 means to inform potentially exposed workers of the existence and location of, and the
67 danger posed by, the spaces. See Appendix A for an example of appropriate hazard
68 signage.

70 (4) When changes in the use or configuration of a non-permit space could result in the need
71 to reclassify the non-permit space as permit space, reassess the hazards in the space and,
72 if necessary, reclassify the space as permit space.

74 (5) If a confined space classified as a permit space poses no actual or potential atmospheric
75 hazards and if all hazards within the space are eliminated without entry into the space, the
76 permit space may be reclassified to a non-permit space for as long as the non-atmospheric
77 hazards remain eliminated.

¹ The requirements of this section apply to workers who enter permit spaces in the conduct of their assigned duties, and their management, i.e., they apply to the OUs.

(6) Note, reference, or include in activity-hazard-review documentation the results of classifications and reclassifications of confined spaces as permit or non-permit spaces.

c. Permit-Space Entry Requirements

One or more of the following set of procedures must be followed for any individual to enter a permit space:

- Procedures for reclassifying a permit space to a non-permit space *for the purpose of entry*; or
- Alternate entry procedures;
- Full-permit entry procedures.

(1) Procedures for Reclassifying a Permit Space to a Non-Permit Space *for the Purpose of Entry*

Non-permit-space entry procedures, i.e., procedures that lie outside the scope of this suborder, may be used to enter a permit space if all of the following conditions are satisfied:

- (a) If the permit space poses no actual or potential atmospheric hazards and if all hazards within the space are eliminated without entry into the space, the permit space may be reclassified to a non-permit space *for the purpose of entry* for as long as the non-atmospheric hazards remain eliminated.
- (b) If it is necessary to enter the permit space to eliminate hazards, such entry shall be performed in accordance with full-permit requirements. If testing and inspection during that entry demonstrate that the hazards within the permit space have been eliminated, the permit space may be reclassified to a non-permit space *for the purpose of entry* for as long as the hazards remain eliminated.
- i. Control of atmospheric hazards through forced-air ventilation does not constitute elimination of the hazards. If it can be demonstrated that forced-air ventilation alone will control all hazards in the space, alternate entry procedures may be used, as indicated above.

- 117 (c) The OU shall document the basis for determining that all hazards in a permit space
118 have been eliminated, through a written certification that contains the following:
119
120 i. Date;
121
122 ii. Space location; and
123
124 iii. Signature of the person making the determination.
125
126 (d) If hazards arise within a permit space that has been reclassified to a non-permit space
127 *for the purpose of entry*, each worker in the space shall exit the space immediately.
128 The space shall then be reevaluated to determine whether it must be reclassified back
129 to a permit space.
130
131 (e) Once entry operations have been completed, the permit space that was reclassified to
132 a non-permit space *for the purpose of entry* shall be reclassified back to a permit
133 space.
134

135 (2) Alternate Entry Procedures

136 Alternate entry procedures may be used to enter a permit space if all of the following
137 conditions are satisfied:
138

- 139 (a) It shall be determined that the only hazard posed by the permit space is an actual or
140 potential hazardous atmosphere.
141
142 (b) It shall be determined that continuous forced-air ventilation alone is sufficient to
143 maintain that the permit space safe for entry.
144
145 (c) These determinations shall be supported by documented monitoring and inspection
146 data.
147
148 i. If an initial entry of the permit space is necessary to obtain the data required, the
149 entry shall be performed using full-permit procedures.
150
151 (d) The determinations and supporting monitoring and inspection data shall be made
152 available to each worker who enters the permit space.
153
154 (e) Entry into the permit space shall be performed in accordance with all of the following
155 requirements, as applicable:
156

- 157 i. Any conditions exterior to the permit space to be entered and making it unsafe to
158 remove an entrance cover shall be eliminated before the cover is removed.
159
- 160 ii. When entrance covers to permit spaces that involve vertical entry are removed,
161 the opening shall be promptly guarded by a railing, temporary cover, or other
162 temporary barrier that will prevent an accidental fall through the opening and
163 that will protect each worker working in the space from foreign objects entering
164 the space.
165
- 166 iii. Before a worker enters the space, the internal atmosphere shall be tested with a
167 calibrated direct-reading instrument for oxygen content and, if applicable,
168 flammable gases/vapors and potential toxic air contaminants, in that order.
169
- 170 (i) Any worker who enters the space shall be provided an opportunity to observe
171 the required pre-entry testing.
172
- 173 (ii) There may be no hazardous atmosphere within the space whenever any
174 worker is inside the space.
175
- 176 (f) Continuous forced-air ventilation shall be used as follows:
177
- 178 i. A worker may not enter the space until the continuous forced-air ventilation has
179 eliminated any hazardous atmosphere.
180
- 181 ii. The continuous forced-air ventilation shall be so directed as to ventilate the
182 immediate areas where a worker is or will be present within the space and shall
183 continue until all workers have left the space.
184
- 185 (i) If the continuous forced-air ventilation stops while entry operations are in
186 progress, all entrants must leave the space immediately.
187
- 188 iii. The air supply for the continuous forced-air ventilation shall be from a clean
189 source and may not increase the hazards in the space.
190
- 191 iv. The atmosphere within the space shall be periodically tested as necessary to
192 ensure that the continuous forced-air ventilation is preventing the accumulation of
193 a hazardous atmosphere.
194
- 195 (i) Any worker who enters the space shall be provided with an opportunity to
196 observe the required periodic testing.

- (g) All of the following steps shall be taken if a hazardous atmosphere is detected during entry:
- i. Each worker shall leave the space immediately.
 - ii. The space shall be evaluated to determine how the hazardous atmosphere developed.
 - iii. Measures shall be implemented to protect workers from the hazardous atmosphere before any subsequent entry takes place.
- (h) It shall be verified that the space is safe for entry and that the pre-entry measures required above have been taken through a written certification that:
- i. Is prepared prior to entry;
 - ii. Contains the date, space location; and signature of the person providing the certification; and
 - iii. Is made available to each worker entering the space.

(3) Full-Permit Entry Procedures

If a permit space cannot be reclassified to a non-permit space *for the purpose of entry* or entered using alternate entry procedures, it must be entered in accordance with the following procedures for full-permit-based entry:

- (a) Implement the measures necessary to prevent unauthorized entry;
- (b) Evaluate and identify the hazards of the permit space before workers enter it;
- (c) Develop and implement the means, procedures, and practices necessary for safe permit space entry operations, including, but is not limited to, the following:
 - i. Specifying acceptable entry conditions;
 - ii. Providing each authorized entrant with the opportunity to observe any monitoring or testing of permit spaces;
 - iii. Isolating the permit space;

- 237 iv. Purging, inerting, flushing, or ventilating the permit space as necessary to
238 eliminate or control atmospheric hazards;
239
240 v. Providing pedestrian, vehicle, or other barriers as necessary to protect entrants
241 from external hazards; and
242
243 vi. Verifying that conditions in the permit space are acceptable for entry throughout
244 the duration of an authorized entry.
245
246 (d) Provide and maintain the following equipment, as necessary to ensure safe entry
247 operations and at no cost to employees, and ensure that workers use it properly:
248
249 i. A meter needed to continuously monitor for oxygen, lower explosive limit or
250 combustible gases/vapors, and, toxic gases/vapors potentially present in the
251 permit space;
252
253 ii. Ventilating equipment needed to obtain acceptable entry conditions;
254
255 iii. Communications equipment;
256
257 iv. PPE insofar as feasible engineering controls and work practice controls do not
258 adequately protect workers;²
259
260 v. Lighting equipment needed to enable workers to see well enough to work safely
261 and to exit the space quickly in an emergency;
262
263 vi. Barriers and shields;
264
265 vii. Equipment, such as ladders, needed for safe ingress and egress by authorized
266 entrants;
267
268 viii. Rescue and emergency equipment; and
269 ix. Any other equipment necessary for safe entry into and rescue from permit
270 spaces.
271
272 (e) Evaluate permit-space conditions as follows when entry operations are conducted:
273
274 i. Test conditions in the permit space to determine if acceptable entry conditions
275 exist before entry is authorized to begin, except that, if isolation of the space is

² PPE is only an option if feasible engineering and work practice controls do not adequately protect workers.

276 infeasible because the space is large or is part of a continuous system (such as a
277 sewer), pre-entry testing shall be performed to the extent feasible before entry is
278 authorized and, if entry is authorized, entry conditions shall be continuously
279 monitored in the areas where authorized entrants are working;
280

281 ii. Test or monitor the permit space as necessary to determine if acceptable entry
282 conditions are being maintained during the course of entry operations;
283

284 iii. Ensure that atmospheric hazards, if any, are monitored in the following
285 chronological order:
286

287 (i) Oxygen;
288

289 (ii) Combustible gases and vapors; and
290

291 (iii) Toxic gases and vapors;
292

293 iv. Provide each authorized entrant an opportunity to observe the pre-entry and any
294 subsequent testing or monitoring of the permit space;
295

296 v. Re-evaluate the permit space in the presence of any authorized entrant who
297 requests re-evaluation because the entrant has reason to believe that the evaluation
298 (i.e., testing/monitoring) of that space may not have been adequate; and
299

300 vi. Immediately provide each authorized entrant with the results of any testing
301 conducted.
302

303 (f) Provide at least one attendant outside the permit space³ into which entry is authorized
304 for the duration of entry operations;
305

306 (g) Designate the person(s) who are to have active roles (as, for example, authorized
307 entrants, attendants, entry supervisors, or persons who test or monitor the atmosphere
308 in a permit space) during entry operations, identify the duties of each person, and
309 provide each worker with training;
310

311 (h) Develop and implement procedures for summoning rescue and emergency services
312 for rescuing entrants from the permit space, for providing necessary emergency

³ If multiple spaces are to be monitored by a single attendant, include in the permit program the means and procedures to enable the attendant to respond to an emergency affecting one or more the permit spaces being monitored without distraction from the attendants responsibilities.

- 313 services to rescued workers, and for preventing unauthorized personnel from
314 attempting a rescue (see Section 6i for additional requirements related to rescue and
315 emergency services);
- 316
- 317 (i) Develop and implement procedures to coordinate entry operations when workers
318 from more than one OU are working simultaneously as authorized entrants in a
319 permit space, so that workers of one OU do not endanger the workers of another OU;
- 320
- 321 (j) Develop and implement procedures, such as closing off the permit space, necessary
322 for concluding the entry after entry operations have been completed;
- 323
- 324 (k) Review entry operations when the OU has reason to believe that the measures taken
325 may not protect workers and correct any deficiencies found in OU planning and
326 implementation of entry operations before subsequent entries are authorized; and
- 327
- 328 (l) Document that the above requirements for full permit-based entry of the permit space
329 have been met by preparing, issuing, using, and cancelling an entry permit meeting
330 the requirements in Section 6d.
- 331
- 332 d. Entry-Permit Requirements
- 333
- 334 (1) Before entry to a permit space is authorized, the OU shall document the completion of
335 measures necessary for entry, as delineated in Section 6c, using an entry permit
336 containing the information specified in 29 CFR 1910.146(f), Entry Permit.
- 337
- 338 (a) The OUs shall use the entry-permit form provided by OSHA, or an alternative form
339 that has been determined by OSHA to contain the required information.
- 340
- 341 (2) Before entry begins, the entry supervisor identified on the permit shall sign the entry
342 permit to authorize entry.
- 343
- 344 (3) So that the entrants can confirm that pre-entry preparations have been completed, the
345 completed permit shall be made available at the time of entry to all authorized entrants by
346 posting it at the entrance to the permit space or by any other equally effective means.
- 347
- 348 (4) The duration of the permit may not exceed the time required to complete the assigned
349 task or job identified on the permit.
- 350
- 351
- 352

(5) The entry supervisor shall terminate entry and cancel the entry permit when:

(a) The entry operations covered by the entry permit have been completed; or

(b) A condition that is not allowed under the entry permit arises in or near the permit space.

(6) Any problems encountered during an entry operation shall be noted on the pertinent permit so that appropriate revisions to OU planning and implementation of entry operations can be made.

e. Review of OU Entry Operations

(1) Review OU entry operations⁴ using the canceled permits retained as required by Section 6h within 1 year after each entry and revise the program as necessary, to ensure that workers participating in entry operations are protected from permit-space hazards.

f. Entry Procedures when Working with Contractors

When an OU arranges to have contractors perform work that involves entry to permit spaces, the OU shall:

(1) Inform the contractor that entry to permit spaces is allowed only through compliance with a permit-space program meeting the requirements of 29 CFR 1910.146;

(2) Apprise the contractor of the elements, including the hazards identified and the OU's experience with the spaces, that make the spaces in question permit spaces;

(3) Apprise the contractor of any precautions or procedures that the OU has implemented for the protection of workers in and near the permit spaces where contractor personnel will be working;

(4) Coordinate entry operations with the contractor when both NIST personnel and contractor personnel will be working in or near the permit spaces; and

(5) Debrief the contractor at the conclusion of entry operations regarding the entry procedures followed and any hazards confronted or created in the permit spaces during entry operations.

⁴ OUs may perform a single annual review covering all entries performed during a 12-month period. If no entry is performed during a 12-month period, no review is necessary.

g. NIST Employees Entering Permit Spaces at Non-NIST Locations

When NIST employees are to enter or be exposed to permit spaces at non-NIST locations, they shall:

(1) Comply with the requirements of this suborder;

(2) Obtain any available information regarding permit-space hazards and past entry operations from the entity responsible for the non-NIST location;

(3) Coordinate entry operations with the entity responsible for the non-NIST location when both NIST employees and others will be working in or near the permit spaces; and

(4) Inform the other entity of the entry procedures that shall be followed; and

(5) Inform the other entity of any hazards confronted or created in the permit spaces, either through a debriefing or during entry operations.

h. Duties of Individuals Involved in Full-Permit-Entry Operations

(1) Authorized entrants shall:

(a) Know the hazards that may be faced during entry, including information on the mode, signs or symptoms, and consequences of the exposure;

(b) Properly use equipment as required by this program;

(c) Communicate with the attendant as necessary to enable the attendant to monitor entrant status and to enable the attendant to alert entrants of the need to evacuate the space as required by this program;

(d) Alert the attendant whenever:

i. The entrant recognizes any warning sign or symptom of exposure to a dangerous situation, or

ii. The entrant detects a prohibited condition;

(e) Exit from the permit space as quickly as possible whenever:

i. An order to evacuate is given by the attendant or the entry supervisor;

- 431 ii. The entrant recognizes any warning sign or symptom of exposure to a dangerous
432 situation;
- 433
- 434 iii. The entrant detects a prohibited condition; or
- 435
- 436 iv. An evacuation alarm is activated.
- 437
- 438 (2) Attendants shall:
- 439
- 440 (a) Know the hazards that may be faced during entry, including information on the mode,
441 signs or symptoms, and consequences of the exposure;
- 442
- 443 (b) Remain aware of possible behavioral effects of hazard exposure in authorized
444 entrants;
- 445
- 446 (c) Continuously maintain an accurate count of authorized entrants in the permit space by
447 name or other means (e.g., through the use of rosters or tracking systems) sufficient to
448 determine quickly and accurately, for the duration the permit, which authorized
449 entrants are in the permit space;
- 450
- 451 (d) Remain outside the permit space during entry operations until relieved by another
452 attendant;
- 453
- 454 (e) Communicate with authorized entrants as necessary to monitor entrant status and to
455 alert entrants of the need to evacuate the space;
- 456
- 457 (f) Monitor activities inside and outside the space to determine if it is safe for entrants to
458 remain in the space and order the authorized entrants to evacuate the permit space
459 immediately if:
- 460
- 461 i. Any of the following are detected:
- 462
- 463 (i) A prohibited condition;
- 464
- 465 (ii) Behavioral effects of exposure of an authorized entrant to a hazard;
- 466
- 467 (iii) A situation outside the space that could endanger the authorized entrants; or
- 468
- 469 ii. Any of the duties assigned to them on entry permits cannot be effectively and
470 safely performed;

- 471 (g) Summon rescue and other emergency services as soon as they have determined that
472 authorized entrants may need assistance to escape from permit-space hazards;
473
- 474 (h) Take the following actions when unauthorized persons approach or enter a permit
475 space while entry is underway:
476
- 477 i. Warn the unauthorized persons that they must stay away from the permit space;
478
- 479 ii. Advise the unauthorized persons that they must exit immediately if they have
480 entered the permit space; and
481
- 482 iii. Inform the authorized entrants and the entry supervisor if unauthorized persons
483 have entered the permit space;
484
- 485 (i) Perform non-entry rescues as specified by the OU's rescue procedure; and
486
- 487 (j) Perform no duties that might interfere with their primary duty to monitor and protect
488 authorized entrants.
489
- 490 (3) Entry supervisors shall:
491
- 492 (a) Know the hazards that may be faced during entry, including information on the mode,
493 signs or symptoms, and consequences of the exposure;
494
- 495 (b) Verify, by checking that the appropriate entries have been made on the permit, that all
496 tests specified by the permit have been conducted and that all procedures and
497 equipment specified by the permit are in place before endorsing the permit and
498 allowing entry to begin;
499
- 500 (c) Terminate entries and cancel entry permits when:
501
- 502 i. Covered entry operations have been completed; or
503
- 504 ii. A condition that is not allowed under the entry permit arises in or near the permit
505 space.
506
- 507 (d) Verify that rescue services are available and that the means for summoning them are
508 operable;
509

- (e) Remove unauthorized individuals who enter or who attempt to enter permit spaces during entry operations; and
- (f) Whenever responsibility for permit-space entry operations is transferred and at intervals dictated by the hazards and operations performed within the space, determine that entry operations remain consistent with the terms of the entry permit and that acceptable entry conditions are maintained.

i. Rescue and Emergency Services

(1) In designating rescue and emergency services in connection with Section 6c(3)(h), OUs shall:

- (a) Evaluate a prospective rescuer's ability to respond to a rescue summons in a timely manner, considering the hazard(s) identified;
- (b) Evaluate a prospective rescue service's ability, in terms of proficiency with rescue-related tasks and equipment, to function appropriately while rescuing entrants from the particular permit space or types of permit spaces identified;⁵
- (c) Select a rescue team or service from those evaluated that:
- i. Has the capability to reach the victim(s) within a time frame that is appropriate for the permit-space hazard(s) identified; and
 - ii. Is equipped for and proficient in performing the needed rescue services;
- (d) Inform each rescue team or service of the hazards they may confront when called on to perform rescue at the site; and
- (e) Provide the rescue team or service selected with access to all permit spaces from which rescue may be necessary so that the rescue service can develop appropriate rescue plans and practice rescue operations.

⁵ What will be considered timely will vary according to the specific hazards involved in each entry. For example, §1910.134, Respiratory Protection, requires that employers provide a standby person or persons capable of immediate action to rescue employee(s) wearing respiratory protection while in work areas defined as IDLH atmospheres.

- (2) An OU whose workers have been designated to provide permit-space rescue and emergency services shall take the following measures:
- (a) Provide affected workers with the PPE needed to conduct permit-space rescues safely and train affected workers so they are proficient in the use of that PPE, at no cost to those employees;
 - (b) Train affected workers to perform assigned rescue duties, including the training required in Section 6k for Authorized Entrants;
 - (c) Train affected workers in basic first-aid and cardiopulmonary resuscitation (CPR);
 - (d) Ensure that at least one member of the rescue team or service holding a current certification in first aid and CPR is available; and
 - (e) Ensure that affected workers practice making permit-space rescues at least once every 12 months, by means of simulated rescue operations in which they remove dummies, manikins, or actual persons from the actual permit spaces or from representative permit spaces that simulate the types of permit spaces from which rescue are to be performed with respect to opening size, configuration, and accessibility.
- (3) To facilitate non-entry rescue, retrieval systems or methods shall be used whenever an authorized entrant enters a permit space, unless the retrieval equipment would increase the overall risk of entry or would not contribute to the rescue of the entrant. Retrieval systems shall meet the following requirements:
- (a) Each authorized entrant shall use a chest or full body harness, with a retrieval line attached at the center of the entrant's back near shoulder level, above the entrant's head, or at another point which the OU can establish presents a profile small enough for the successful removal of the entrant. Wristlets may be used in lieu of the chest or full body harness if the OU can demonstrate that the use of a chest or full body harness is infeasible or creates a greater hazard and that the use of wristlets is the safest and most effective alternative.
 - (b) The other end of the retrieval line shall be attached to a mechanical device or fixed point outside the permit space in such a manner that rescue can begin as soon as the rescuer becomes aware that rescue is necessary. A mechanical device shall be available to retrieve personnel from vertical type permit spaces more than 5 feet (1.52 m) deep.

(4) If an injured entrant is exposed to a substance for which a Material Safety Data Sheet or other similar written information is required to be kept at the worksite, that information shall be made available to the medical facility treating the exposed entrant.

j. Records (Other than Training Records)

(1) OUs shall retain each canceled entry permit for at least 1 year to facilitate the review of entry operations.

k. Training

(1) Training of Individuals Who Are to Reclassify Permit Spaces to a Non-Permit Spaces *for the Purpose of Entry* or Use Alternate Entry Procedures

(a) Such individuals shall complete the following prior to reclassifying permit spaces or engaging in alternate entry operations:

- i. The one-time-only training provided by OSHE on the NIST Permit-Required Confined Spaces program; and
- ii. The activity-specific training required by hazard reviews applicable to the work to be conducted and sufficient to establish their proficiency to conduct that work.

(b) The activity-specific training for such individuals shall be provided by individuals who have successfully completed training on the NIST Permit-Required Confined Spaces program and who are familiar with entry operations for the activity-specific space or a representative space.

(2) Training of Individuals Who Are to Use Full-Permit Entry Procedures

(a) Authorized Entrants, Attendants, and Entry Supervisors shall complete the following prior to engaging in full-permit entry operations:

- i. The one-time-only training provided by OSHE on the Permit-Required Confined Spaces program; and
- ii. The activity-specific training required by hazard reviews applicable to the work to be conducted, including training on their respective duties as delineated in Section 6h, and sufficient to establish their proficiency to conduct that work.

(b) The activity-specific training for Authorized Entrants, Attendants, and Entry Supervisors shall be provided by individuals who have successfully completed training on the NIST Permit-Required Confined Spaces program and who have demonstrated their proficiency in entry operations representative of those that the Authorized Entrants, Attendants, and Entry Supervisors are to conduct.

(3) Training of Official First-Level Supervisors of Individuals Involved in Entry Operations, Regardless of the Entry Procedures to be Used

(a) The one-time-only training provided by OSHE on the NIST Permit-Required Confined Spaces program.

(4) Additional Activity-Specific Training of Individuals Involved in Entry Operations, Regardless of the Entry Procedures to be Used

(a) Additional activity-specific training of such individuals must be conducted under the following conditions:

- i. Before there is a change in assigned duties;
- ii. Whenever there is a change in permit-space operations that presents a hazard about which a worker has not previously been trained; or
- iii. Whenever the OU has reason to believe either that there are deviations from permit-space entry procedures or that there are inadequacies in the worker's knowledge or use of these procedures.

(b) The training shall introduce, and establish worker proficiency in, new or revised procedures, as necessary.

(5) Documentation and Recording of Activity-Specific Training

(a) OUs shall document activity-specific training and record its completion by affected employees in accordance with OU procedures.

(b) Training records must, at a minimum, contain the following information and be available for inspection by workers and their authorized representatives:

- i. Each worker's name;

- 664 ii. Trainer's signature(s); and
665
666 iii. Training dates.
667
- 668 1. Employee Participation
669
- 670 (1) OUs shall consult with affected employees and their authorized representatives on the
671 development and implementation of all aspects of the NIST Permit-Required Confined
672 Spaces program.
673
- 674 (2) OUs shall make available to affected employees and their authorized representatives all
675 information required by the NIST Permit-Required Confined Spaces program.
676
677
- 678 **7. DEFINITIONS**
- 679 a. Acceptable Entry Conditions – The conditions that must exist in a permit space to allow
680 entry and to ensure that workers involved with a permit-space entry can safely enter into and
681 work within the space.
682
- 683 b. Attendant – An individual stationed outside one or more permit spaces who monitors the
684 authorized entrants and who performs all attendant's duties assigned in the entry permit.
685
- 686 c. Authorized Entrant – An employee who is authorized by the employer to enter a permit
687 space.
688
- 689 d. Blanking or Blinding – The absolute closure of a pipe, line, or duct by the fastening of a solid
690 plate (such as a spectacle blind or a skillet blind) that completely covers the bore and that is
691 capable of withstanding the maximum pressure of the pipe, line, or duct with no leakage
692 beyond the plate.
693
- 694 e. Confined Space – A space that:
695
- 696 (1) Is large enough and so configured that a worker can bodily enter and perform assigned
697 work; and
698
- 699 (2) Has limited or restricted means for entry or exit, as in the case of some tanks, vessels,
700 silos, storage bins, hoppers, vaults, and pits); and
701
- 702 (3) Is not designed for continuous occupancy.
703

- f. Double Block and Bleed – The closure of a line, duct, or pipe by closing and locking or tagging two in-line valves and by opening and locking or tagging a drain or vent valve in the line between the two closed valves.
- g. Emergency – Any occurrence (including any failure of hazard control or monitoring equipment) or event internal or external to the permit space that could endanger entrants.
- h. Engulfment – The surrounding and effective capture of a person by a liquid or finely divided (flowable) solid substance that can be aspirated to cause death by filling or plugging the respiratory system or that can exert enough force on the body to cause death by strangulation, constriction, or crushing.
- i. Entry – The action by which a person passes through an opening into a permit space. Entry is considered to have occurred as soon as any part of the entrant's body breaks the plane of an opening into the space.⁶
- j. Entry Operations – The activities that take place in a permit space once that space has been entered.
- k. Entry Permit (Permit) – The written or printed document that is provided by the employer to allow and control entry into a permit space and containing the information specified in 29 CFR 1910.146(f), Entry Permit.
- l. Entry Supervisor – The person (such as the employer, foreman, or crew chief) responsible for determining if acceptable entry conditions are present at a permit space where entry is planned, for authorizing entry and overseeing entry operations, and for terminating entry as required by this section.⁷
- m. Hazardous Atmosphere – An atmosphere that may expose workers to the risk of death, incapacitation, impairment of ability to self-rescue (that is, escape unaided from a permit space), injury, or acute illness from one or more of the following causes:
- (1) Flammable gas, vapor, or mist in excess of 10 percent of its lower flammable limit (LFL);

⁶ This definition does not apply to spaces that are too small to accommodate an entire body. For example, it would not apply to a hand or fingers breaking the plane to turn a knob if the space were not large enough to accommodate the entire body.

⁷ An entry supervisor also may serve as an attendant or as an authorized entrant as long as that person is trained and equipped as required by this suborder for each role he or she fills. Also, the duties of entry supervisor may be passed from one individual to another during the course of an entry operation.

- (2) Airborne combustible dust at a concentration that meets or exceeds its LFL;⁸
- (3) Atmospheric oxygen concentration below 19.5 percent or above 23.5 percent;
- (4) Atmospheric concentration of any substance for which a dose or a permissible exposure limit is published in Subpart G, Occupational Health and Environmental Control, or in Subpart Z, Toxic and Hazardous Substances, of 29 CFR 1910 and which could result in worker exposure in excess of its dose or permissible exposure limit;⁹ and
- (5) Any other atmospheric condition that is immediately dangerous to life or health.¹⁰

- n. Hot-Work Permit – The employer's written authorization to perform operations (for example, riveting, welding, cutting, burning, and heating) capable of providing a source of ignition.
- o. Immediately Dangerous to Life or Health (IDLH) – Any condition that poses an immediate or delayed threat to life or that would cause irreversible adverse health effects or that would interfere with an individual's ability to escape unaided from a permit space.¹¹
- p. Inerting – The displacement of the atmosphere in a permit space by a noncombustible gas (such as nitrogen) to such an extent that the resulting atmosphere is noncombustible. This procedure produces an IDLH oxygen-deficient atmosphere.
- q. Isolation – The process by which a permit space is removed from service and completely protected against the release of energy and material into the space by such means as blanking or blinding; misaligning or removing sections of lines, pipes, or ducts; a double block and bleed system; lockout or tagout of all sources of energy; or blocking or disconnecting all mechanical linkages.
- r. Line Breaking – The intentional opening of a pipe, line, or duct that is or has been carrying flammable, corrosive, or toxic material, an inert gas, or any fluid at a volume, pressure, or temperature capable of causing injury.

⁸ This concentration may be approximated as a condition in which the dust obscures vision at a distance of 5 feet (1.52 m) or less.

⁹ An atmospheric concentration of any substance that is not capable of causing death, incapacitation, impairment of ability to self-rescue, injury, or acute illness due to its health effects is not covered by this provision.

¹⁰ For air contaminants for which OSHA has not determined a dose or permissible exposure limit, other sources of information, such as Material Safety Data Sheets that comply with the Hazard Communication Standard, 29 CFR 1910.1200, published information, and internal documents can provide guidance in establishing acceptable atmospheric conditions.

¹¹ Some materials -- hydrogen fluoride gas and cadmium vapor, for example -- may produce immediate transient effects that, even if severe, may pass without medical attention, but are followed by sudden, possibly fatal collapse 12-72 hours after exposure. The victim "feels normal" from recovery from transient effects until collapse. Such materials in hazardous quantities are considered to be "immediately" dangerous to life or health.

- s. Non-Permit-Required Confined Space – A confined space that does not contain or, with respect to atmospheric hazards, have the potential to contain, any hazard capable of causing death or serious physical harm.
- t. Non-Permit Space – See “Non-Permit-Required Confined Space”.
- u. Oxygen-Deficient Atmosphere – An atmosphere containing less than 19.5 percent oxygen by volume.
- v. Oxygen-Enriched Atmosphere – An atmosphere containing more than 23.5 percent oxygen by volume.
- w. Permit-Required Confined Space – A confined space that has one or more of the following characteristics:
- (1) Contains or has a potential to contain a hazardous atmosphere;
 - (2) Contains a material that has the potential for engulfing an entrant;
 - (3) Has an internal configuration such that an entrant could be trapped or asphyxiated by inwardly converging walls or by a floor which slopes downward and tapers to a smaller cross-section; or
 - (4) Contains any other recognized serious safety or health hazard.
- x. Permit Space – See “Permit-Required Confined Space.
- y. Prohibited Condition – Any condition in a permit space that is not allowed by the permit during the period when entry is authorized.
- z. Rescue Service – The personnel designated to rescue workers from permit spaces.
- aa. Retrieval System – The equipment (including a retrieval line, chest or full-body harness, wristlets, if appropriate, and a lifting device or anchor) used for non-entry rescue of persons from permit spaces.

- bb. Testing – The process by which the hazards that may confront entrants of a permit space are identified and evaluated. Testing includes specifying the tests that are to be performed in the permit space.¹²

8. ACRONYMS

- a. CFR – Code of Federal Regulations
- b. CPR – Cardiopulmonary Resuscitation
- c. IDLH – Immediately Dangerous Life or Health
- d. LFL – Lower Flammable Limit
- e. OSH – Occupational Safety and Health
- f. OSHA – Occupational Safety and Health Administration
- g. OSHE – Office of Safety, Health, and Environment
- h. OU – Organizational Unit
- i. PPE – Personal Protective Equipment

9. ROLES AND RESPONSIBILITIES

- a. The OUs are responsible for ensuring that the requirements in Section 6 are met.

10. AUTHORITIES

There are no authorities specific to this suborder alone.

11. DIRECTIVE OWNER

Chief Safety Officer

¹² Testing enables employers both to devise and implement adequate control measures for the protection of authorized entrants and to determine if acceptable entry conditions are present immediately prior to, and during, entry.

843	12. APPENDICES
844	a. Examples of Required Hazard Signage
845	
846	

847

Appendix A. Examples of Required Hazard Signage



848

849



850

851

Respiratory Protection

NIST S 7101.58

Document Approval Date: 03/20/2014

Effective Date: 04/01/2015

1. PURPOSE

The purpose of the Respiratory Protection Program (RPP) is to prevent NIST employees from breathing airborne hazards when effective engineering controls are not feasible. In addition, the program identifies required training and practices for selecting, using, caring for, and storing respiratory protection.

2. BACKGROUND

- a. NIST must meet or exceed the requirements established by the Occupational Safety and Health Administration (OSHA) in [29 Code of Federal Regulations \(CFR\) 1910.134](#), Respiratory Protection. Implementation of this suborder through the requirements in Section 6 and the roles and responsibilities in Section 9 exceeds those requirements.
- b. This suborder supersedes NIST Health and Safety Instruction (HSI) 17, Respiratory Protection, October 1998.

3. APPLICABILITY

The provisions of this suborder apply to all NIST employees whose exposure to potential airborne hazards could result in their being required to wear, or their voluntarily wearing, respiratory protection to carry out their assigned duties.

4. REFERENCES

- a. [29 CFR 1910.134](#), Respiratory Protection.
- b. [29 CFR 1910.1020](#), Access to Employee Exposure and Medical Records.
- c. ANSI Z88.2, American National Standard for Respiratory Protection.

- d. ANSI Z88.6, American National Standard for Respiratory Protection – Respirator Use Physical Qualifications for Personnel.
- e. Compressed Gas Association (CGA) Commodity Specification for Air, CGA G7.1.
- f. NFPA 1500, Standard on Fire Department Occupational Safety and Health Program.
- g. NFPA 1852, Standard on Selection, Care, and Maintenance of Open-Circuit Self-Contained Breathing Apparatus (SCBA).
- h. NFPA 1981, Standard on Open-Circuit Self-Contained Breathing Apparatus (SCBA) for Emergency Services.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews;
- b. NIST S 7101.21: Personal Protective Equipment;
- c. NIST S 7101.23: Safety Education and Training; and
- d. NIST S 7101.22: Hazard Signage.

6. REQUIREMENTS¹

When effective engineering controls are not feasible, or while they are being implemented, respirators must be used to (a) reduce exposures to airborne hazards to levels below applicable occupational exposure limits (OELs), and (b) protect against exposures to atmospheres that are “immediately dangerous to life or health” (IDLH)². Specific respiratory-protection requirements include the occupational exposure limits adopted by NIST; hazard identification; hazard assessment; control methods, including respiratory protection selected by competent persons; respirator medical evaluations; respirator fit testing; respirator use; respirator maintenance and care; breathing air quality; entry and work in IDLH atmospheres; records (other than training records); training; and communication.

¹ The requirements in this section apply to employees who wear respiratory protection in the conduct of their assigned duties, and their management, i.e., they apply to the OUs.

² Instances of IDLH atmospheres outside of the Office of Facilities and Property Management and emergency situations would be highly unusual. Only highly-trained personnel may enter or prepare to enter atmospheres known or considered to be IDLH. For additional information, contact OSHE.

a. OELs and IDLH Atmospheres

(1) Employees shall not be exposed to airborne hazards within the personal breathing zone (PBZ) at levels that exceed the OELs adopted by NIST.

(2) The OELs adopted by NIST shall be the permissible exposure limits established by OSHA or the following exposure limits, when these limits are more stringent than those established by OSHA and achieving them is feasible:

(a) Threshold Limit Values established by the American Conference of Governmental Industrial Hygienists; or

(b) Exposure limits established by other authoritative entities, such as the National Institute of Occupational Safety and Health (NIOSH)

(3) Unprotected employees shall not be exposed to IDLH atmospheres.

b. Hazard Identification

(1) If a concern arises³ regarding potential airborne hazards in an already ongoing activity, a consultation shall be scheduled with a competent person as soon as possible to determine if the airborne hazards could result in exposures that exceed an applicable OEL or could create an IDLH atmosphere.

(2) If the hazard review of a new activity identifies potential airborne hazards, a consultation shall be scheduled with a competent person to determine if the airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere.

(3) If the hazard review of a change in an existing activity identifies new airborne hazards or potential increases in previously identified airborne hazards, a consultation shall be scheduled with a competent person to determine if the airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere.

c. Hazard Assessment

(1) If the consultation with the competent person indicates that airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere, arrangements

³ Such a concern could be raised by any individual, e.g., a worker, a coworker, a supervisor, a Division Safety Representative, or a competent person.

shall be made for a competent person to assess the hazards using exposure monitoring, mathematical calculations, or other means.

- (2) If the competent person cannot identify or reasonably estimate the employee's potential exposure, the atmosphere shall be considered IDLH.

d. Control Methods

- (1) When it has been determined by a competent person that, without controls, airborne hazards *would result* in potential exposures that exceed an OEL or constitute an atmosphere known or considered to be IDLH:

(a) Feasible⁴ engineering controls shall be implemented in an effort to reduce the level of airborne hazards in the PBZ to less than applicable OELs or to mitigate the atmosphere known or considered to be IDLH.

(b) If the implementation of feasible engineering controls fails to achieve the desired objectives, as determined by a competent person, respiratory protection selected by a competent person shall be provided and used to reduce potential exposures to airborne hazards within the PBZ to less than applicable OELs or to prevent potential exposures to the atmosphere known or considered to be IDLH.⁵

(c) Only respirators selected by the competent person shall be procured.

(d) All respirators, cartridges, filters, and other components shall be provided at no cost to employees.

- (2) When it has been determined by a competent person that, without controls, airborne hazards *would not result* in exposures that exceed an OEL or constitute an IDLH atmosphere:

(a) Feasible engineering controls should be implemented in an effort to reduce exposures to airborne hazards in the PBZ.

⁴ Feasible means that the OEL is both technologically and economically achievable. Technologically feasible means that there is a reasonable possibility that the agency will be able to meet the OEL in most of its operations by installing engineering controls and implementing work practice controls. Technologically feasible also includes being able to use analytical techniques to measure the airborne hazard at the OEL. For a Federal agency, economically feasible means that complying with the OEL will not require such resources as to threaten the agency's ability to fulfill its mission.

⁵ Many precautions in addition to respiratory protection are necessary for employees other than first responders to enter atmospheres known or considered to be IDLH. For further information, contact OSHE.

- (b) Respiratory protection may be worn voluntarily if it is determined, based on a consultation with a competent person, that:
- i. Such protection will not in itself create a more serious safety or health hazard;
 - ii. The respiratory protection is selected by a competent person;
 - iii. Use of the respiratory protection is authorized by the employee's Official First-Level Supervisor; and
 - iv. Use of the respiratory protection complies with the requirements of this suborder.

e. Respirator Medical Evaluations

- (1) All employees who are to wear respirators, except filtering facepieces worn voluntarily, shall arrange for the Health Unit⁶ to complete a medical evaluation prior to fit testing.
- (2) Additional medical evaluations are required under the following circumstances:
 - (a) Employees report medical signs or symptoms related to the ability to use a respirator;
 - (b) The Health Unit, the OSHA Respiratory Protection Program Manager, or the Official First-Level Supervisor recommends reevaluation;
 - (c) Information from the Respiratory Protection program, including observations made during fit testing and program evaluations, indicates a need; or
 - (d) A change occurs in workplace conditions, e.g., in physical work effort, protective clothing required, or temperature, that may substantially increase the physiological burden on an employee.

f. Fit Testing

- (1) After receiving medical evaluations, employees who are to wear respirators with tight-fitting facepiece shall complete fit testing provided by a competent person:
 - (a) Prior to initial use of the respirator and at least annually thereafter;

⁶ "Provided by the Health Unit" means "provided by a physician or other licensed health-care professional working in the Health Unit".

(b) Pursuant to any change, authorized by a competent person, in respirator make, model, style, or size; and

(c) Pursuant to a change in employee facial shape/structure (dentures, weight gain, facial hair, broken nose, glasses/goggles) that could prevent a good face seal or interfere with the respirator's ability to function properly.

(2) If an employee needs prescription eyewear, regardless of the mask type, he or she must be provided with the appropriate eyewear and respirator type to accommodate that..

g. Respirator Use

(1) All respirators, cartridges, filters, and other procured components shall be used in accordance with manufacturers' specifications.

(2) Labels on filters, cartridges, and canisters shall not be removed and must remain legible.

(3) Cartridges or canisters shall be changed in accordance with the change schedule provided by the competent person or sooner if users feel ill or breakthrough occurs.

(4) Tight-fitting respirators shall not be worn when conditions prevent a good face seal or interfere with the respirator's ability to function properly. Such conditions may include facial hair between the sealing surface of the facepiece and the face, or facial hair that interferes with valve function. Other conditions that may prevent a good face seal include, but are not limited to, scars, absence of teeth/dentures, unusual facial configurations, or wearing objects that project under the facepiece (e.g., corrective glasses or goggles).

(5) Tight-fitting-respirator users shall be monitored⁷ by their supervisors for face-to-facepiece seal conditions, and those with interfering conditions shall not be permitted to perform work that requires the use of a respirator.

(6) Seal checks of tight-fitting respirators shall be performed by users prior to use in accordance with [29 CFR Part 1910.134, Appendix B-1](#), User Seal Check Procedures (Mandatory).⁸

⁷ That is, if a supervisor observes or becomes aware that an employee who wears a tight-fitting facepiece has a beard or other factor preventing a tight seal between the face and respirator, the supervisor shall not permit the employee to wear the respirator.

⁸ User seal checks are not a substitute for fit tests.

(7) Respirators shall not be loosened or removed in work situations where their use is required.

(8) Respirator users shall leave the respirator use area:

(a) To wash their face and facepiece as necessary to prevent eye or skin irritation associated with respirator use;

(b) If they detect vapor or gas breakthrough, changes in breathing resistance, or leakage of the facepiece;

(c) If they feel ill or disoriented; and

(d) To replace the respirator or filter, cartridge, or canister elements.

h. Respirator Maintenance and Care

(1) Cleaning

(a) When practicable, respirators should be assigned to individual employees for their exclusive use. Permanently assigned respirators can be marked with an indelible marker or in a similar manner that does not affect performance.

(b) Exclusive-use respirators shall be cleaned and disinfected as often as necessary to maintain them in a sanitary condition.

(c) Shared-use respirators shall be cleaned and disinfected by the user after each use.

(d) Emergency-use respirators shall be cleaned and disinfected after each use.

(e) All respirators shall be cleaned prior to storage.

(f) Respirators shall be cleaned and disinfected in accordance with [29 CFR 1910.134, Appendix B-2](#), Respirator Cleaning Procedures (Mandatory).

(2) Storage

(a) Respirators shall be stored in accordance with the manufacturers' specifications.

(b) All respirators shall be stored to protect them from damage, contamination, dust, sunlight, extreme temperatures, excessive moisture, and damaging chemicals.

(c) All respirators shall be stored to prevent deformation of the facepiece and exhalation valve, and as such should not be stored in such places as lockers or tool boxes unless they are in carrying cases or otherwise protected from damage.

(d) Emergency-use respirators shall be stored in the work area in clearly marked, quickly accessible, protective containers, and in an adequate number in each area in which they may be needed.

(3) Inspection

(a) All respirators used in routine situations shall be inspected before each use and during cleaning.

(b) Respirator inspections shall include the following, as applicable to the respirator being used:

i. A check of respirator function, tightness, and connections;

ii. A check of the condition of the various parts, including, but not limited to, the facepiece; head straps; valves; connecting tube; and cartridges, canisters or filters; and

iii. A check of elastomeric parts for pliability and signs of deterioration.

(c) Emergency-Use Respirators

i. All emergency-use respirators shall be inspected at least monthly and in accordance with the manufacturers' recommendations.

ii. All emergency-use respirators shall be checked for proper function before and after each use.

iii. Emergency escape-only respirators shall be inspected before being carried into the workplace.

iv. Emergency-use respirator inspections shall document the following information:

- (i) Date the inspection was performed;
- (ii) Name of the person who performed it;
- (iii) Findings;
- (iv) Any required remedial action; and
- (v) A serial number or other means of identifying the inspected respirator.

v. Emergency-use respirator inspections shall be documented:

- (i) On tags or labels that are attached to the respirators or kept within their storage compartments; or
- (ii) In inspection reports stored in hard copy or electronic form.

(d) SCBAs

i. In addition to the requirements in Section h(3)(a), (b), and (c)i-iii:

- (i) SCBAs shall be inspected monthly.
- (ii) Air and oxygen cylinders shall be maintained in a fully charged state and shall be recharged when the pressure falls to 90% of the manufacturer's specified pressure level.
- (iii) Regulators and warning devices shall be inspected to determine that they function properly.
- (iv) Inspection tags shall be attached to SCBA storage units and tamper-evident seals should be affixed to the storage units to indicate whether they have been opened.

ii. If SCBAs are maintained for emergency use, inspections shall be documented in accordance with the requirements in Sections h(3)(c)iv-v.

338 (4) Repairs

339
340 (a) Respirators that fail an inspection or are found to be defective shall be removed from
341 service immediately, marked or tagged as out of service, and discarded or repaired.

342
343 (b) Particulate filters shall be replaced when they become soiled or damaged or users
344 detect increased breathing resistance.

345
346 (c) Respirator repairs or adjustments are to be made only by appropriately trained
347 persons and shall use only the respirator manufacturer's parts designed for that
348 respirator.

349
350 i. Reducing and admission valves, regulators, and alarms shall be adjusted or
351 repaired only by the manufacturer or by a manufacturer-trained technician.

352
353 (d) Repairs shall be made according to manufacturers' specifications for the type and
354 extent of repairs to be made.

355
356 i. Respirator Maintenance and Care – Additional Requirements for SCBAs Used in
357 Firefighting (*applicable to the NIST Fire Protection Group only*)

358
359 (1) SCBAs used in firefighting must comply with the additional requirements of NFPA 1500,
360 Fire Department Occupational Safety and Health Program Standard, including the
361 following guidelines:

362
363 (a) NFPA 1852, Selection, Care, and Maintenance of Open-Circuit Self-Contained
364 Breathing Apparatus (SCBA) Standard.

365
366 (b) NFPA 1852, Chapter 6, on the care, cleaning, and storage of SCBA equipment.

367
368 (c) NFPA 1852, Chapter 7, on inspecting and maintaining of SCBAs.

369
370 i. SCBAs assigned to on-duty NIST employees must be inspected at the beginning
371 of each duty shift.

372
373 ii. SCBAs which are on duty assignment, but not currently assigned to an individual
374 employee, must be inspected weekly.

375
376 iii. In all cases, SCBAs must be inspected, at a minimum, on a weekly basis.

- 378 iv. If the SCBA incorporates an integrated Personal Alert Safety System (PASS), it
379 also must be inspected as part of the SCBA inspection at the beginning of each
380 duty shift while assigned to an employee or weekly if the SCBA is not assigned to
381 an individual duty employee.
382
- 383 (d) NFPA 1981, Chapter 4, on flow testing of SCBAs.
384
- 385 i. SCBAs shall be flow tested at least annually.
386
- 387 j. Breathing Air Quality in SCBAs and Airline Respirators
388
- 389 (1) Compressed breathing air procured by the OUs shall meet at least the requirements for
390 Grade D breathing air described in ANSI/Compressed Gas Association Commodity
391 Specification for Air, G-7.1-1989.
392
- 393 (2) Cylinders supplying breathing air shall meet Department of Transportation requirements
394 ([Requirement for DOT Specification Cylinders](#)) and have certificates of analysis that
395 show they meet or exceed Grade D breathing-air requirements.
396
- 397 (3) Compressors supplying breathing air shall be constructed and situated in a way that
398 prevents entry of contaminated air into the air-supply system.
399
- 400 k. Entry and Work in IDLH Atmospheres
401
- 402 (1) For entry and work in atmospheres known or considered to be IDLH, the following
403 procedures shall be followed:
404
- 405 (a) A minimum of one employee shall be located outside the IDLH atmosphere.
406
- 407 i. The use of two employees inside the work area and two employees outside the
408 work area is recommended.
409
- 410 (b) Visual, voice, or signal line communication shall be maintained between employees
411 in the IDLH atmosphere and employees located outside the IDLH atmosphere.
412
- 413 (c) Employees located outside the IDLH atmosphere shall be trained and equipped to
414 provide effective emergency rescue.
415
- 416 (d) A supervisor or designee shall be notified before employees outside the IDLH
417 atmosphere enter to provide emergency rescue.

(e) In addition to having the respiratory protection selected by a competent person, employees trained to provide emergency rescue in IDLH atmospheres⁹ shall be equipped with pressure-demand or positive-pressure SCBAs, or a positive-pressure supplied-air respirator with auxiliary SCBA, and have either the appropriate retrieval equipment for removing individuals from the IDLH atmosphere (such as a retrieval line or a chest or full-body harness), or an equivalent means of rescue when retrieval equipment is not available.

(2) For interior structural firefighting, the following procedures shall be followed in addition to those in Section I(1) (*applicable to the NIST Fire Protection Group only*):

(a) Firefighters shall only enter the IDLH atmosphere in pairs and shall remain in visual or voice contact with one another at all times.

(b) At least two firefighters shall be located outside the IDLH atmosphere the entire time firefighters are within it.

i. One of the two firefighters located outside the IDLH atmosphere may be assigned to an additional role, such as incident commander in charge of the emergency or safety officer, so long as the individual is able to perform assistance or rescue activities without jeopardizing the safety or health of any firefighter working at the incident.

(c) Firefighters may perform emergency rescue activities before an entire team has assembled.

I. Records (Other than Training Records)

(1) Results of hazard assessments conducted by competent persons of potential airborne hazards or IDLH atmospheres shall be noted, referenced, or included as part of the activity-hazard-review documentation.

(2) Records¹⁰ of monthly inspections of emergency-use respirators, including emergency-use SCBAs, shall be maintained until replaced following a subsequent inspection.

⁹ To provide emergency rescue in IDLH atmospheres, individuals would require a high level of training in specialized emergency response. Such training is outside the scope of this suborder. For additional information, contact OSHA.

¹⁰ The records referenced in Sections 6n(2)-(6) could take the form of tags, labels, or reports.

- 453 (3) Records of inspections of emergency escape-only respirators prior to their being carried
454 into the workplace shall be maintained.
- 455 (4) Records of quarterly air-quality testing for air supplied via compressors shall be
456 maintained until replaced following a subsequent air-quality test.
- 457
- 458 (5) Records of annual flow testing of all SCBAs shall be maintained until replaced following
459 a subsequent flow test.
- 460
- 461 (6) Records of weekly inspections of SCBAs used in firefighting shall be maintained until
462 replaced following a subsequent inspection.
- 463

464 m. Training

465

- 466 (1) Employees required to wear respirators, or who voluntarily wear respirators other than
467 filtering facepieces, shall complete:
- 468

469 (a) Training provided by OSHE on the applicable elements of the RPP;

470

471 (b) Retraining provided by OSHE on the applicable elements of the RPP at least
472 annually; and

473

474 (c) Retraining identified by the Official First-Level Supervisor whenever:

475

476 i. Changes in the workplace or in the type of respirator render training obsolete;

477

478 ii. Inadequacies in the employee's knowledge or use of the respirator indicate the
479 need for retraining; or

480

481 iii. Any other situation arises in which retraining appears necessary to ensure safe
482 respirator use.

483

- 484 (2) Employees who voluntarily wear filtering facepieces shall complete:
- 485

486 (a) Training provided by OSHE on the applicable elements of the RPP.

487

- 488 (3) Official First-Level Supervisors of employees required to wear respirators, or who
489 voluntarily wear respirators other than filtering facepieces, shall complete training
490 provided by OSHE on the elements of the RPP applicable to the employees they
491 supervise.
- 492

(4) Training shall be documented and recorded in accordance with the requirements, roles, and responsibilities in the Safety Education and Training suborder.

n. Communication

(1) Hazard signage shall be posted at entrances to areas in which respiratory protection is required. Appendix A provides an example of hazard signage meeting these requirements.

(2) Electronic or hard copies of this suborder and of [29 CFR 1910.134](#) shall be made available to affected employees.

7. DEFINITIONS

a. Airborne Exposure – Exposure to a concentration of an airborne contaminant that would occur if the employee were not using respiratory protection.

b. Airborne Hazard – Breathing air contaminated with harmful dusts, fogs, fumes, mists, gases, smokes, sprays, or vapors.

c. Air-Purifying Respirator – A type of respirator with an air-purifying filter, canister or cartridge, which removes specific air contaminants by passing ambient air through the air-purifying element.

d. Atmosphere-Supplying Respirator – A respirator that supplies the user with breathing air from a source independent of the ambient atmosphere, and includes supplied-air respirators (SARs), and self-contained breathing apparatus (SCBA) units.

e. Canister or Cartridge – Container with a filter, sorbent, catalyst, or combination of these items that removes specific contaminants from the air passed through the container.

f. Competent Person – A CIH or CSP in the NIST Office of Safety, Health and Environment (OSHE) or another NIST Organizational Unit (OU), a consultant CIH or CSP, or an individual directed by a CIH or CSP, who is capable of anticipating, recognizing, controlling, and evaluating potential occupational hazards.

g. Certified Industrial Hygienist (CIH) – An individual who is board certified by the American Board of Industrial Hygiene and has met the minimum requirements for education experience, and through examination has demonstrated a minimum level of knowledge in occupational health subject areas such as respiratory protection.

- h. Certified Safety Professional (CSP) – An individual who is board certified by the Board of Certified Safety Professionals and has met the professional challenge of demonstrating competency through education, experience, and examination.
- i. Dust Mask – See Filtering Facepiece.
- j. Escape-Only Respirator – A respirator intended to be used only for emergency exit.
- k. Filtering Facepiece – Also referred to as a dust mask, is a negative pressure particulate respirator with a particulate filter as an integral part of the facepiece or with the entire facepiece composed of the filtering media.
- l. Filter – A component used in respirators to remove solid or liquid aerosols from the inspired air.
- m. Fit Test – Protocol to quantitatively or qualitatively evaluate the fit of a tight-fitting respirator on an individual.
- n. Immediately Dangerous to Life or Health (IDLH) – An atmosphere that poses an immediate threat to life, would cause irreversible adverse health effects, or would impair an individual's ability to escape from a dangerous atmosphere. An atmosphere is considered IDLH when the airborne hazard cannot be identified, reasonably estimated, or the atmosphere is oxygen deficient (<19.5% oxygen by volume).
- o. Loose-Fitting Facepiece – A respiratory inlet covering designed to form a partial seal with the face.
- p. Occupational Exposure Limit (OEL) – An upper limit on the acceptable concentration of a hazardous substance in workplace air for a particular material or class of materials.
- q. Personal Breathing Zone (PBZ) – The zone encompassing the nose and mouth and a hemisphere forward of the shoulders with a radius of 6 to 9 inches (~ 1 foot sphere, with nose being at the center of the sphere).
- r. Potential Airborne Hazard – A hazard with the potential to become airborne within the PBZ or to create an IDLH atmosphere.
- s. Powered Air-Purifying Respirator (PAPR) – A positive-pressure air-purifying respirator that uses a blower to force the ambient air through air-purifying elements to the inlet covering.

- t. Respiratory Inlet Covering – That portion of a respirator that forms the protective barrier between the user’s respiratory tract and an air-purifying device, or breathing air source, or both.
- u. Self-Contained Breathing Apparatus (SCBA) – An atmosphere-supplying respirator for which the breathing air source is designed to be carried by the user.
- v. Supplied-Air Respirator (SAR) or Airline Respirator – An atmosphere-supplying respirator for which the source of breathing air is not designed to be carried by the user.
- w. Tight-Fitting Facepiece – A respiratory inlet covering that forms a complete seal with the face.

8. ACRONYMS

- a. CGA – Compressed Gas Association
- b. NFPA – National Fire Protection Association
- c. NIOSH – The National Institute for Occupational Safety and Health
- d. OSHA – Occupational Safety and Health Administration
- e. OSHE – Office of Safety, Health, and Environment
- f. OU – Organizational Unit
- g. PBZ – Personal Breathing Zone
- h. RPP – Respiratory Protection Program

9. ROLES AND RESPONSIBILITIES

- a. Employees Engaged in Activities Involving Airborne Hazards that Could Result in Exposures that Exceed an OEL or Could Create an IDLH Atmosphere:

- (1) If a concern arises regarding potential airborne hazards in an already ongoing activity, schedule a consultation with a competent person as soon as possible to determine if the airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere;

- (2) If the hazard review of a new activity identifies potential airborne hazards, schedule a consultation with a competent person to determine if the airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere;
- (3) If the hazard review of a change in an existing activity identifies new airborne hazards, or potential increases in previously identified airborne hazards, schedule a consultation with a competent person to determine if the airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere;
- (4) Inform Official First-Level Supervisors of any consultations scheduled with competent persons and of the results of those consultations;
- (5) If consultation with a competent person indicates that airborne hazards could result in exposures that exceed an OEL or could create an IDLH atmosphere, arrange for a competent person to assess the airborne hazards;
- (6) When it has been determined by a competent person that, without controls, airborne hazards *would result* in potential exposures that exceed an OEL or constitute an atmosphere known or considered to be IDLH, implement feasible engineering controls in an effort to reduce the level of airborne hazards in the PBZ to less than applicable OELs or to mitigate the atmosphere known or considered to be IDLH;
- (7) If feasible engineering controls fail to achieve the desired objectives, use respiratory protection selected by a competent person to reduce potential exposures to airborne hazards within the PBZ to less than applicable OELs or to prevent potential exposures to the atmosphere known or considered to be IDLH;¹¹ and
- (8) Ensure that the results of hazard assessments, i.e., the results of consultations, including the results of exposure monitoring, mathematical calculations, or other means used to assess the airborne hazards, are noted, referenced, or included as part of the activity-hazard-review documentation.

b. Employees Required to Wear Respirators, or Who Voluntarily Wear Respirators Other than Filtering Facepieces (in addition to the responsibilities of above):

- (1) Obtain medical evaluations in accordance with the requirements in Section 6e;
- (2) Obtain fit tests in accordance with the requirements in Section 6f, if applicable;

¹¹ Many precautions in addition to respiratory protection are necessary for employees other than first responders to enter atmospheres known or considered to be IDLH. For additional information, contact OSHE.

- 650 (3) Use, maintain, and care for the respirators provided by their Official First-Level
651 Supervisors in accordance with the requirements in Section 6g, 6h, and 6i, as applicable,
652 and their training as specified in Section 6m;
653
654 (4) Ensure that breathing air meets the requirements in Section 6j, if applicable;
655
656 (5) Enter and conduct work in IDLH atmospheres in accordance with the procedures in
657 Section 6k, if applicable;
658
659 (6) Complete the training specified in Section 6m, as assigned by their Official First-Level
660 Supervisors; and
661
662 (7) Request additional training as duties change or as otherwise needed.
663

664 c. Employees Who Voluntarily Wear Filtering Facepieces:
665

- 666 (1) Complete the training specified in Section 6m, as assigned by their Official First-Level
667 Supervisor.
668

669 d. Official First-Level Supervisors of Any of the Above Employees:
670

- 671 (1) Ensure that competent persons from outside of OSHE engaged by the OU to conduct
672 hazard assessments, select respiratory protection, or provide fit testing understand the
673 responsibilities delineated below for competent persons;
674
675 (2) Provide the results of hazard assessments resulting in employees they supervise being
676 required to wear respiratory protection, or resulting in their voluntarily wearing
677 respiratory protection, to all such affected employees, the OSHE RPP Manager, and the
678 Health Unit for inclusion in employee medical files;
679
680 (3) Ensure that the results of hazard assessments are noted, referenced, or included as part of
681 the activity-hazard-review documentation;
682
683 (4) Make electronic or hard copies of this suborder and of [29 CFR 1910.134](#) available to
684 employees they supervise who are required to, or voluntarily, wear respiratory
685 protection;
686
687 (5) Provide affected employees with the respiratory protection selected by a competent
688 person, at no cost to affected employees;
689

- 690 (6) Authorize the voluntary use of respirators by employees they supervise;
691
692 (7) Ensure that records, other than training records, are maintained in accordance with the
693 requirements in Section l;
694
695 (8) Assign training to the affected employees they supervise in accordance with the
696 requirements in Section 6m and do so when:
697
698 (a) Employees enter on duty;
699
700 (b) Employees' duties change; and
701
702 (c) Special circumstances arise such as those indicated in Section 6m(1)(c).
703
704 (9) Ensure that training specified in Section 6m(1)(c) is documented and recorded in
705 accordance with the requirements, roles, and responsibilities in the Safety Education and
706 Training suborder;
707
708 (10) If employees they supervise are required to wear respirators, or are to voluntarily wear
709 respirators other than filtering facepieces, complete the training specified in Section 6m
710 for Official First-Level Supervisors; and
711
712 (11) Ensure that hazard signage meeting the requirements in Section 6n is posted at entrances
713 to areas in which respiratory protection is required.
714

715 e. Chief Safety Officer:
716

- 717 (1) Assign an OSHE employee to serve as the OSHE Safety Program Manager for the RPP at
718 both the Gaithersburg and Boulder sites.¹²
719

720 f. OSHE Respiratory Protection Program Manager:
721

- 722 (1) Administer the RPP in accordance with the requirements of [29 CFR 1910.134](#);
723
724 (2) Ensure that electronic or hard copies of this suborder and of [29 CFR 1910.134](#) are made
725 available to the Health Units;
726

¹² The OSHE Respiratory Protection Program Manager shall carry out the roles of "Program Administrator" identified in 29 CFR 1910.134.

- 727 (3) Retain all fit-testing records until the next required fit tests have been administered and
728 received and make such records available to affected employees upon request;
729
730 (4) Ensure that affected employees are notified when annual fit testing and training are due;
731
732 (5) Ensure that training provided by OSHE on the RPP is available and meets the
733 requirements of 29 CFR 1910.134(k), Training and Information;
734
735 (6) Ensure that training provided by OSHE on the RPP is documented in NIST's electronic
736 safety training application;
737
738 (7) Ensure that non-web-based training provided by OSHE on the RPP and completed by
739 affected employees is recorded in NIST's electronic safety training application;
740
741 (8) Assist NIST staff in the development of signage that complies with the requirements of
742 this suborder and the NIST Hazard Signage Program; and
743
744 (9) Implement procedures to evaluate program effectiveness.
745

746 g. Competent Persons:
747

- 748 (1) Consult with employees to determine if airborne hazards could result in exposures that
749 exceed an applicable OEL or could create an IDLH atmosphere;
750
751 (2) When airborne hazards could result in exposures that exceed an applicable OEL or could
752 create an IDLH atmosphere, conduct exposure monitoring or use mathematical
753 calculations or other means to assess the hazard, document the results in writing, and
754 provide those results to the employee who scheduled the assessment and his or her
755 Official First-Level Supervisor within 15 working days after the receipt of the results or
756 within the time frame specified in any applicable substance-specific OSHA standard;
757
758 (3) When it has been determined that employees must wear respiratory protection:
759
760 (a) Specify the necessary protection in accordance with 29 CFR 1910.134(d), Selection
761 of Respirators;
762
763 (b) Provide the Health Unit with the following information:
764
765 i. The type and weight of the respirator to be used;
766

- 767 ii. The duration and frequency of respirator use (including use for rescue and
768 escape);
769
770 iii. The expected physical work effort;
771
772 iv. Additional protective clothing and equipment to be worn; and
773
774 v. Temperature and humidity extremes that may be encountered;
775
776 (4) Provide employees who have completed their medical examinations with fit testing in
777 accordance with 29 CFR 1910(f), Fit Testing;
778
779 (a) Provide fit-testing records to the OSHE RPP Manager.
780

781 h. Health Units:

- 782
783 (1) Administer a respiratory-protection medical evaluation program in accordance with 29
784 CFR 1910.134(e), Medical Evaluation, and 29 CFR 1910.1020, Access to Employee
785 Exposure and Medical Records.
786
787

788 **10. AUTHORITIES**

789 There are no authorities specific to this suborder alone.
790
791

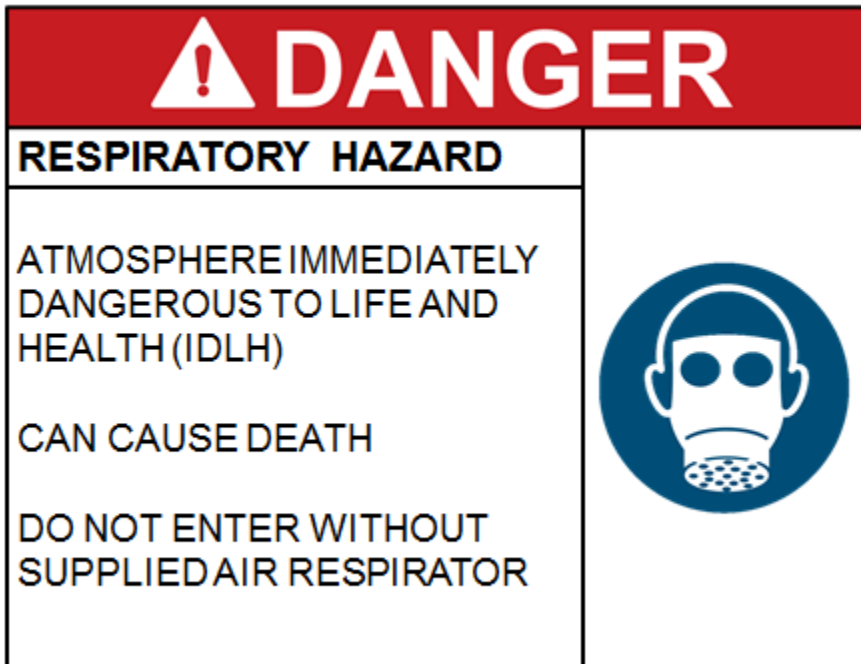
792 **11. DIRECTIVE OWNER**

793 Chief Safety Officer.
794
795

796 **12. APPENDICES**

797 a. Hazard Signage
798
799

800 Appendix A. Hazard Signage
801



802
803

CHEMICAL HAZARD COMMUNICATION

NIST S 7101.59

Approval Date: 02/08/2016

Deployment Start Date: 02/08/2016

Effective Date:¹ 06/01/2016 for Training and Workplace Labeling Requirements
10/01/2016 for All Other Program Requirements

1. PURPOSE

The purpose of the NIST Chemical Hazard Communication Program is to ensure that the hazards of all chemicals resident at or shipped from a NIST workplace (see definition of “NIST Workplace”) are classified and communicated to potentially exposed employees, covered associates², and other parties. This suborder also serves as NIST’s written hazard communication program, as required by Occupational Safety and Health Administration (OSHA) Hazard Communication Standard 29 CFR 1910.1200 (HCS).

2. BACKGROUND

The HCS was promulgated in 1994 to ensure that the hazards of all chemicals produced or imported are classified and that information concerning the classified hazards is transmitted to employers and employees. The HCS was revised in 2012 to align with the United Nations Globally Harmonized System of Classification and Labelling of Chemicals (GHS), Revision 3 and provide a common and coherent approach to classifying chemicals and communicating hazard information.

¹ For revision history, see Appendix A.

² The terms “Associate” and “Covered Associate” are defined as follows in [NIST Order \(O\) 7101.00: Occupational Safety and Health Management System](#): “Associate” – An individual conducting work at NIST who is not a NIST employee. For a list of NIST associate types, click [here](#). “Covered Associate” – A NIST associate who performs work at a NIST workplace in accordance with NIST safety requirements. Covered associates include Foreign and Domestic Guest Researchers (including contractors who perform NIST R&D/technical work); Research Associates; Intergovernmental Agency Personnel Act assignees; Facility Users; Volunteer Students; and DOC employees who work at NIST workplaces.

The HCS requires chemical manufacturers and importers to classify the hazards of chemicals that they produce or import and to provide information about the chemical hazards through labels on shipped containers and more detailed information sheets called safety data sheets (SDSs).

The HCS requires employers to develop and implement a written hazard communication program, which describes how the employer will comply with the HCS requirements for preparing and distributing SDSs, labeling containers of chemicals in the workplace and containers being shipped to other workplaces, maintaining a list of the hazardous chemicals known to be present in the workplace, informing employees of the hazards of non-routine tasks, informing employees of the hazards associated with chemicals in unlabeled pipes in the workplace, providing employee training regarding chemical hazards and protective measures, and communicating chemical hazard information to other employers.

This suborder supersedes NIST Administrative Manual Subchapter 12.17, *Chemical Hazard Communication*, NIST Health and Safety Instruction # 7, *Hazard Communication*, and NIST Health and Safety Instruction # 15, *Chemical Container Labeling*.

3. APPLICABILITY

a. The provisions of this suborder apply to all NIST workplaces and to all NIST employees and covered associates who may be exposed to hazardous chemicals under normal conditions of use or in a foreseeable emergency (see definition of “Foreseeable Emergency”).

b. The provisions of this suborder apply to:

(1) Any chemical known to be present in a NIST workplace in such a manner that NIST employees or covered associates could be exposed under normal conditions of use or in a foreseeable emergency;³ and

(2) Hazardous chemicals shipped from a NIST workplace.

c. Hazardous chemicals exempt from specific *labeling requirements* of this suborder⁴ include:

(1) Any pesticide as such term is defined in the Federal Insecticide, Fungicide, and Rodenticide Act (7 U.S.C. 136 et seq.), when subject to the labeling requirements of that

³ Chemicals within the scope of other NIST OSH suborders (e.g., compressed gases, cryogenics) shall comply with the applicable requirements of this and any other applicable NIST OSH suborder.

⁴ Hazardous chemicals exempt from specific labeling requirements of this suborder shall be labeled in accordance with the labeling requirements of the applicable Act and regulations.

Act and labeling regulations issued under that Act by the Environmental Protection Agency;

(2) Any chemical substance or mixture as such terms are defined in the Toxic Substances Control Act (15 U.S.C. 2601 et seq.), when subject to the labeling requirements of that Act and labeling regulations issued under that Act by the Environmental Protection Agency;

(3) Any food, food additive, color additive, drug, cosmetic, or medical or veterinary device or product, including materials intended for use as ingredients in such products (e.g. flavors and fragrances), as such terms are defined in the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301 et seq.) or the Virus-Serum-Toxin Act of 1913 (21 U.S.C. 151 et seq.), and regulations issued under those Acts, when they are subject to the labeling requirements under those Acts by either the Food and Drug Administration or the Department of Agriculture;

(4) Any distilled spirits (beverage alcohols), wine, or malt beverage intended for nonindustrial use, as such terms are defined in the Federal Alcohol Administration Act (27 U.S.C. 201 et seq.) and regulations issued under that Act, when subject to the labeling requirements of that Act and labeling regulations issued under that Act by the Bureau of Alcohol, Tobacco, Firearms and Explosives;

(5) Any consumer product or hazardous substance as those terms are defined in the Consumer Product Safety Act (15 U.S.C. 2051 et seq.) and Federal Hazardous Substances Act (15 U.S.C. 1261 et seq.) respectively, when subject to a consumer product safety standard or labeling requirement of those Acts, or regulations issued under those Acts by the Consumer Product Safety Commission; and,

(6) Agricultural or vegetable seed treated with pesticides and labeled in accordance with the Federal Seed Act (7 U.S.C. 1551 et seq.) and the labeling regulations issued under that Act by the Department of Agriculture.

d. Hazardous chemicals exempt from all requirements of this suborder are detailed in 29 CFR 1910.1200(b)(6). These exemptions include, but are not limited to:

(1) Hazardous waste⁵;

(2) Tobacco or tobacco products;

⁵ Hazardous wastes at a NIST workplace shall comply with the requirements of NIST S 7301.4, *Hazardous Waste Accumulation*.

- (3) Wood or wood products which have not been treated with a hazardous chemical covered by this standard, and wood which will not be subsequently sawed or cut, generating dust;
- (4) Articles (see definition of “Article”);
- (5) Food, beverages, drugs, and cosmetics intended for personal consumption in the workplace;
- (6) Any consumer product that is used in the workplace for the purpose intended by the manufacturer or importer of the product and the use of which results in a duration and frequency of exposure that is not greater than the range of exposures that could reasonably be experienced by consumers when used for the purpose intended;
- (7) Nuisance particles where the chemical manufacturer can establish that they do not pose any physical or health hazard;
- (8) Ionizing and non-ionizing radiation⁶; and,
- (9) Biological hazards⁷.

4. REFERENCES

- a. OSHA 29 CFR 1910.1200, *Hazard Communication in General Industry*
- b. OSHA 29 CFR 1910.1001, *Asbestos*
- c. OSHA 29 CFR 1910.1003, *13 Carcinogens*
- d. OSHA 29 CFR 1910.1017, *Vinyl Chloride*
- e. OSHA 29 CFR 1910.1018, *Inorganic Arsenic*
- f. OSHA 29 CFR 1910.1025, *Lead*
- g. OSHA 29 CFR 1910.1026, *Chromium (VI)*
- h. OSHA 29 CFR 1910.1027, *Cadmium*

⁶ Chemical hazards associated with sources of ionizing and non-ionizing radiation are not exempted from the requirements of this program.

⁷ Chemical hazards associated with biological hazards are not exempted from the requirements of this program.

- i. OSHA 29 CFR 1910.1028, *Benzene*
 - j. OSHA 29 CFR 1910.1029, *Coke Oven Emissions*
 - k. OSHA 29 CFR 1910.1044, *1,2-Dibromo-3-Chloropropane*
 - l. OSHA 29 CFR 1910.1045, *Acrylonitrile*
 - m. OSHA 29 CFR 1910.1047, *Ethylene Oxide*
 - n. OSHA 29 CFR 1910.1048, *Formaldehyde*
 - o. OSHA 29 CFR 1910.1050, *Methylenedianiline*
 - p. OSHA 29 CFR 1910.1051, *1,3-Butadiene*
 - q. OSHA 29 CFR 1910.1052, *Methylene Chloride*
 - r. OSHA 29 CFR 1910.1201, *Retention of DOT Markings, Placards, and Labels*
 - s. OSHA 29 CFR 1910.1450, *Occupational Exposure to Hazardous Chemicals in Laboratories*
 - t. OSHA 29 CFR 1926.59, *Hazard Communication in Construction*
 - u. OSHA 3371-08 2009, *Hazard Communication Guidance for Combustible Dusts*
- 5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS**
- a. NIST S 7101.60: *Chemical Management (Chemical Hygiene Plan)*
 - b. NIST S 7101.61: *Compressed Gas Safety*
 - c. NIST S 7101.28: *Contractor Safety*
 - d. NIST S 7101.52: *Cryogen Safety*
 - e. NIST S 7101.54: *Dispersible Engineered Nanomaterials*
 - f. NIST S 7101.21: *Personal Protective Equipment*

g. NIST S 7101.29: *Procurement Safety*

h. NIST S 7101.23: *Safety Education and Training*

i. NIST S 7101.20: *Work and Worker Authorization Based on Hazard Reviews*

6. REQUIREMENTS

The requirements in this section address the issue of determining and classifying the potential hazards of chemicals resident at or shipped from a NIST workplace and communicating information concerning their hazards to employees, associates, and other parties. Some of the requirements in this suborder (e.g., chemical hazard classifications, SDSs, and training) may be integral to or result from the conduct of hazard reviews in accordance with NIST S 7101.20: *Work and Worker Authorization Based on Hazard Reviews* when the activity under review involves hazardous chemicals.

a. Chemical Hazard Determinations and Classifications (required for potentially Hazardous Chemicals)

Chemical Hazard Determination is the process of identifying relevant data regarding the hazards of a chemical; reviewing the data to ascertain the hazards associated with the chemical by comparing the data with the criteria specified in the HCS for health and physical hazards; and deciding whether the chemical will be classified as hazardous (see definition of “Hazardous Chemical”).

Chemical Hazard Classification is a Chemical Hazard Determination with an additional determination of the degree of each health and physical hazard, where appropriate, by comparing the data with the criteria specified in the HCS for health and physical hazards.

(1) General Requirements

(a) Chemical hazard determinations and classifications shall be performed as early as possible, preferably prior to the chemical being produced or used.

(b) Chemical hazard determinations and classifications shall follow the procedures described in 29 CFR 1910.1200 - Appendices A and B to determine and classify the hazards of the chemicals, including determinations regarding when chemical mixtures are covered. When determining or classifying chemical mixtures produced or imported by NIST employees or associates, the information provided on the current SDSs of the individual ingredients may be relied upon, except where it is known or in

the exercise of reasonable diligence should have been known that the SDS misstates or omits information required by 29 CFR 1910.1200.

(c) Chemical hazard determinations and classifications shall identify and consider the full range of available scientific literature and other evidence concerning the potential hazards and shall consult:

i. 29 CFR 1910.1200-Appendix A regarding health hazards,

ii. 29 CFR 1910.1200-Appendix B regarding physical hazards,

iii. 29 CFR 1910.1200(c) regarding simple asphyxiant, pyrophoric gas, and hazard not otherwise classified (see definition “Hazard Not Otherwise Classified”) hazards, and

iv. 3371-08 2009 - *Hazard Communication Guidance for Combustible Dusts* regarding combustible dust hazards.

(d) Chemical hazard determinations shall determine all hazard classes described in 29 CFR 1910.1200 that apply to the chemical being classified.

(e) Chemical hazard classifications shall determine all hazard classes⁸ and, where appropriate, the category of each hazard class described in 29 CFR 1910.1200 that apply to the chemical being classified.

(f) Chemical hazard classifications for chemicals regulated by OSHA in the Chemical-Specific Health Standards shall be performed in compliance with the procedures described in the OSHA Chemical-Specific Health Standards, when applicable (see Appendix B of this suborder).

(g) Chemical hazard classifications shall be described in writing and include a description of the classification process, any relevant data regarding the chemical hazards, and a description of the basis of determination for any assigned hazard

⁸ HCS(2012) hazard classes include: acute toxicity, skin corrosion or irritation, serious eye damage or eye irritation, respiratory or skin sensitization, germ cell mutagenicity, carcinogenicity, reproductive toxicity, specific target organ toxicity, aspiration hazard, simple asphyxiant, explosive, flammable, oxidizer, self-reactive, pyrophoric, self-heating, organic peroxide, corrosive to metal, gas under pressure, in contact with water emits flammable gas, combustible dust, and hazards not otherwise classified (HNOC); some HCS(2012) hazard classes include additional criteria (e.g., route or frequency of exposure, physical state of chemical); see HCS(2012) for complete hazard class information.

- 253 classes and, where appropriate, the category of each hazard class described in 29 CFR
254 1910.1200 that apply to the chemical being classified.
- 255
- 256 (2) Hazardous Chemicals at a NIST Workplace whose Use at that Workplace Meets the
257 Definition of “Laboratory Use”
- 258
- 259 (a) Chemical hazard classifications shall be conducted for chemicals acquired at a NIST
260 workplace that will be shipped from the NIST workplace, whenever the chemical
261 users decide that the results of the chemical hazard classifications contained in the
262 SDSs obtained from the suppliers shall not be relied upon⁹ *and when SDSs were not*
263 *provided by the suppliers.*
- 264
- 265 (b) *Chemical hazard determinations shall be conducted for chemicals acquired at a NIST*
266 *workplace that will not be shipped from the NIST workplace, whenever the chemical*
267 *users decide that the results of the chemical hazard classifications contained in the*
268 *SDSs obtained from the suppliers shall not be relied upon and when SDSs were not*
269 *provided by the suppliers.*
- 270
- 271 (c) Chemical hazard classifications shall be conducted for chemicals produced at a NIST
272 workplace that will be shipped from the NIST workplace.
- 273
- 274 (d) *Chemical hazard determinations shall be conducted for chemicals produced at a*
275 *NIST workplace that will not be shipped from the NIST workplace.*
- 276
- 277 (3) Hazardous Chemicals at a NIST Workplace whose Use at that Workplace Does Not Meet
278 the Definition of “Laboratory Use”
- 279
- 280 (a) Chemical hazard classifications shall be conducted for chemicals acquired at a NIST
281 workplace, whenever the chemical users decide that the results of the chemical hazard
282 classifications contained in the SDSs obtained from the suppliers shall not be relied
283 upon¹⁰.
- 284
- 285 (b) Chemical hazard classifications shall be conducted for chemicals produced at a NIST
286 workplace.
- 287
- 288

⁹ Chemical manufacturers should be contacted to communicate any discrepancies in the obtained SDSs and to request revised SDSs.

¹⁰ Chemical manufacturers should be contacted to communicate any discrepancies in the obtained SDSs and to request revised SDSs.

b. Safety Data Sheets (required for Hazardous Chemicals)

(1) General Requirements

- (a) SDSs shall include the same product identifier, name, address, and telephone number of the chemical manufacturer, importer, or other responsible party used on the container label.
- (b) SDSs shall be in English.
- (c) SDSs developed by or on behalf of employees or covered associates shall contain the section numbers and section headings in the order specified in 29 CFR Part 1910.1200(g)(2) and include the information specified in 29 CFR Part 1910.1200-Appendix D.
 - i. If no relevant information is found for any sub-heading within a section on the SDS, the SDS shall be marked to indicate that no applicable information was found.
- (d) SDSs developed by or on behalf of employees or covered associates shall contain information that accurately reflects the scientific evidence used in the associated Chemical Hazard Classifications.
- (e) SDSs developed by or on behalf of employees or covered associates shall be revised within 3 months of employees or covered associates becoming newly aware of any significant information regarding the hazards of a chemical, or ways to protect against the hazards. The revised SDS shall be provided with all future shipped containers of the chemical. If the chemical is not currently being produced or imported at the NIST workplace, the SDS shall be revised before the chemical is introduced into or shipped from the NIST workplace again.
- (f) SDSs for each hazardous chemical listed on a Hazardous Chemical Inventory List shall be readily accessible in the work area electronically¹¹ or in hard copy during each work shift when employees or covered associates are present.
- (g) SDSs shall be readily available upon request and in accordance with the requirements of 29 CFR 1910.1020(e).

¹¹ “Readily accessible in the work area electronically” means that employees and covered associates can access SDSs on a NIST information-technology system in the work area.

- 327 (2) Hazardous Chemicals at a NIST Workplace whose Use at that Workplace Meets the
328 Definition of “Laboratory Use”
329
- 330 (a) SDSs received with incoming shipments shall be maintained and readily accessible in
331 the work area electronically or in hard copy during each work shift when employees
332 or covered associates are present.
333
- 334 (b) SDSs shall be developed for chemicals acquired at a NIST workplace that will be
335 shipped from the NIST workplace, whenever the chemical users decide that the
336 results of the chemical hazard classifications contained in the SDSs obtained from the
337 suppliers shall not be relied upon¹² and when SDSs were not provided by the
338 suppliers.
339
- 340 (c) SDSs shall be developed for chemicals produced at a NIST workplace that will be
341 *shipped* from the NIST workplace.
342
- 343 (3) Hazardous Chemicals at a NIST Workplace whose Use at that Workplace Does Not Meet
344 the Definition of “Laboratory Use”
345
- 346 (a) SDSs received with incoming shipments shall be maintained and readily accessible in
347 the work area electronically or in hard copy during each work shift when employees
348 or covered associates are present. *If an SDS was not provided with a shipment and not*
349 *already possessed at the time of delivery, the SDS shall be obtained from the supplier*
350 *as soon as possible.*
351
- 352 (b) SDSs shall be developed for chemicals acquired at a NIST workplace that will be
353 shipped from the NIST workplace, whenever the chemical users decide that the
354 results of the chemical hazard classifications contained in the SDSs obtained from the
355 suppliers shall not be relied upon¹³.
356
- 357 (c) SDSs shall be developed for chemicals produced at a NIST workplace.
358
359
360
361
362

¹² Chemical manufacturers should be contacted to communicate any discrepancies in the obtained SDSs and to request revised SDSs.

¹³ Chemical manufacturers should be contacted to communicate any discrepancies in the provided SDSs and to request revised SDSs.

(4) Hazardous Chemicals Shipped from a NIST Workplace

- (a) SDSs shall be provided with the initial shipment and upon request to each recipient. If the SDS has been revised, the revised SDS shall be provided with the first shipment to each recipient that occurs after the SDS has been revised.

c. Labels and Other Forms of Warning

(1) General Requirements

- (a) Labels and other forms of warning shall be prominently displayed.
- (b) Labels and other forms of warning shall be in English, legible, and contain information that is current.
- (c) Labels and other forms of warning shall be revised within 6 months of employees or covered associates becoming newly aware of significant information regarding the hazards of a chemical. The revised label shall be provided with all future shipped containers of the chemical. If the chemical is not currently present at the NIST workplace, labels and other forms of warning shall be revised before the chemical is introduced into or shipped from the NIST workplace again.

(2) Hazardous Chemicals at a NIST Workplace

- (a) Hazardous chemical containers shall be labeled, tagged, or marked with¹⁴:

EITHER

i. Shipped Container Label Information

- (i) Product identifier;
- (ii) Signal word, hazard statement(s), pictogram(s), and precautionary statement(s) in accordance with the requirements of 29 CFR 1910.1200-Appendix C, for each hazard class and associated hazard category for the hazardous chemical;

¹⁴ Hazardous chemicals at a NIST workplace exempt from specific labeling requirements of this suborder shall be labeled in accordance with the labeling requirements of the applicable Act and regulations (see Section 3c) and include the NIST Chemical Owner Name.

(iii) Name, address, and telephone number of the chemical manufacturer, importer, or other responsible party; and,

(iv) NIST Chemical Owner Name¹⁵.

OR

ii. Workplace Container Label Information

(i) Product identifier;

(ii) Words, pictures, symbols, or combination thereof, which provide at least general information regarding the hazards of the chemicals, and which, in conjunction with the other information immediately available under NIST S 7101.59: *Chemical Hazard Communication*, will provide employees and covered associates with the specific information regarding the physical and health hazards of the hazardous chemical; and

(iii) NIST Chemical Owner Name¹⁶.

(b) Existing labels on chemical containers entering a NIST workplace shall not be removed or defaced, unless the containers are immediately marked, labeled, or tagged with the required information¹⁷.

(c) Alternate methods of labeling (e.g., signs, placards, process sheets, batch tickets, operating procedures, or other such written materials) may be used in lieu of affixing labels to individual stationary process containers¹⁸, as long as the alternative method:

i. Identifies the containers to which it is applicable;

¹⁵ SRMs stored under the control of the Office of Reference Materials (ORM) are not required to be labeled with the NIST Chemical Owner Name.

¹⁶ SRMs stored under the control of the ORM are not required to be labeled with the NIST Chemical Owner Name.

¹⁷ If the acquired container no longer contains the originally-acquired chemical or the results of a chemical hazard classification identify that the existing label information is not current, the container should be re-marked, re-labeled or re-tagged to indicate the required label information for the current contents of the container. If the container is "Empty", it is recommended that a line be drawn through the original label and the container should be marked with the word "Empty" to indicate that the original chemical is no longer present.

¹⁸ In certain "Laboratory Use" situations (e.g., when the container is too small to provide all required label elements), the Alternate Methods of Labeling may be employed for containers in the NIST workplace that are not stationary process containers; when feasible to do so, such containers shall be labeled with at least the Workplace Container Label Information [see Section 6c(2)(a)(ii)].

- 429
- 430 ii. Conveys the information required to be on a label in accordance with Section
- 431 6c(2)(a) of this suborder; and
- 432
- 433 iii. Is readily accessible to the employees and covered associates in their work area
- 434 throughout each work shift.
- 435
- 436 (d) Portable containers into which hazardous chemicals are transferred from labeled
- 437 containers, and which are intended only for the immediate use (see definition of
- 438 “Immediate Use”) of the employee or covered associate who performs the transfer,
- 439 may be labeled but are not required to be.
- 440
- 441 (3) Hazardous Chemicals Shipped from a NIST Workplace
- 442
- 443 (a) Each hazardous chemical container leaving the NIST workplace shall be labeled,
- 444 tagged, or marked with the following in a manner which does not conflict with the
- 445 requirements of the Hazardous Materials Transportation Act (49 U.S.C. 1801 et seq.)
- 446 and regulations issued under that Act by the Department of Transportation¹⁹:
- 447
- 448 i. Product identifier;
- 449
- 450 ii. Signal word, hazard statement(s), pictogram(s), and precautionary statement(s) in
- 451 accordance with the requirements of 29 CFR 1910.1200-Appendix C, for each
- 452 hazard class and associated hazard category for the hazardous chemical; and
- 453
- 454 iii. Name, address, and telephone number of the chemical manufacturer, importer, or
- 455 other responsible party. If the hazardous chemical was produced by NIST, the
- 456 container shall be labeled, tagged, or marked with:
- 457
- 458 (i) National Institute of Standards and Technology;
- 459
- 460 (ii) NIST Responsible Party Name (i.e., OU/Division Name);
- 461
- 462 (iii) NIST Responsible Party Address (i.e., OU/Division Address); and,
- 463
- 464 (iv) NIST Responsible Party Telephone Number (i.e., OU/Division Telephone
- 465 Number for the NIST employee or covered associate who has been designated

¹⁹ Hazardous chemicals exempt from specific labeling requirements of this suborder shall be labeled in accordance with the labeling requirements of the applicable Act and regulations (see Section 3c).

to provide additional information on the hazardous chemical and appropriate emergency procedures, if necessary.)²⁰.

- (b) The signal word, hazard statement(s), pictogram(s), and precautionary statement(s) shall be located together on the container label, tag, or mark.

(4) Non-Hazardous Chemicals at a NIST Workplace

- (a) Non-Hazardous chemical containers should be labeled, tagged, or marked with:

- i. Product identifier; and,
- ii. NIST Chemical Owner Name²¹.

d. Hazardous Chemical Inventory Lists²² (required for Hazardous Chemicals)

- (1) Hazardous Chemicals at a NIST Workplace whose Use at that Workplace Meets the Definition of “Laboratory Use”

- (a) Hazardous Chemical Inventory Lists shall be prepared and list all commercially-acquired hazardous chemicals²³ present in OU-assigned work areas.
- (b) Hazardous Chemical Inventory Lists shall include the product identifiers that are referenced on the corresponding container labels and SDSs of the hazardous chemicals present in OU-assigned work areas.

²⁰ SRMs stored under the control of the ORM may be labeled with “National Institute of Standards and Technology”, the NIST Gaithersburg address, and the NIST Responsible Party Telephone Number to meet this requirement.

²¹ SRMs stored under the control of the ORM are not required to be labeled with the NIST Chemical Owner Name.

²² Hazardous chemicals that are owned by a NIST employee or covered associate shall be inventoried in CISPro. In select situations [e.g., Hollings inventory, SRMs stored under the control of the ORM], hazardous chemicals may be inventoried outside of CISPro; in such situations, OSHE shall be notified of the inventories and the Hazardous Chemical Inventory Lists shall be made readily available upon request electronically or in hard copy. It is recommended that in work areas in which individuals other than NIST employees or covered associates are conducting work (“multi-employer work areas”) or in work areas where not all of the hazardous chemicals are inventoried in CISPro, a master Hazardous Chemical Inventory List that represents all hazardous chemicals in the work area be printed and posted. Hazardous chemicals that are Biohazardous Materials or LC-RAM shall satisfy the CHC inventory requirements in accordance with the requirements specified in this program. Hazardous chemicals that are SNM-362 RAM shall satisfy the CHC inventory requirements in accordance with the requirements specified in NIST S 7201.01, Ionizing Radiation Safety – Radioactive Material at NIST Gaithersburg.

²³ Hazardous-chemical SRMs labeled for sale by NIST that are sold or transferred by ORM to employees or covered associates outside of ORM shall be considered commercially-acquired hazardous chemicals.

(c) Hazardous Chemical Inventory Lists shall be maintained and made readily available upon request electronically or in hard copy.

(2) Hazardous Chemicals at a NIST Workplace whose Use at that Workplace Does Not Meet the Definition of “Laboratory Use”

(a) Hazardous Chemical Inventory Lists shall be prepared and list all hazardous chemicals present in OU-assigned work areas.

(b) Hazardous Chemical Inventory Lists shall include the product identifiers that are referenced on the corresponding container labels and SDSs of the hazardous chemicals present in OU-assigned work areas.

(c) Hazardous Chemical Inventory Lists shall be maintained and made readily available upon request electronically or in hard copy.

e. Hazardous Activities

(1) The chemical hazards of routine and non-routine activities performed by NIST employees and covered associates shall be communicated to all NIST employees and covered associates who may be exposed to the hazardous chemicals in accordance with the training requirements of this suborder and the requirements of NIST S 7101.20: *Work and Worker Authorization Based on Hazard Reviews*.

f. Hazardous Chemicals in Pipes

(1) The identities and hazards of hazardous chemicals located inside of pipes shall be communicated to all NIST employees and covered associates who may be exposed to the hazardous chemicals under normal conditions of use or in a foreseeable emergency (see definition of “Foreseeable Emergency”) in accordance with the training requirements of this suborder and the requirements of NIST S 7101.20: *Work and Worker Authorization Based on Hazard Reviews*.

g. Information and Training

(1) Training shall be provided, documented, and recorded in accordance with the requirements of the NIST S 7101.23: *Safety Education and Training*.

(2) All employees and covered associates to whom this suborder applies shall be provided with effective information and training on the hazardous chemicals in their work areas.

Information and training may be designed to cover categories of hazards (e.g., flammability, carcinogenicity) or specific chemicals; however, chemical-specific information must always be available through labels and other forms of warning and SDSs.

(3) All employees and covered associates to whom this suborder applies shall receive the following training at the time of their initial assignment to a NIST workplace:

(a) Training provided by OSHE on the details of this suborder, covering the following topics:

- i. The requirements of 29 CFR 1910.1200;
- ii. The location, availability, and requirements of this suborder, including the Hazardous Chemical Inventory List, Container Labeling and Other Forms of Warning, and SDSs required by this suborder and 29 CFR 1910.1200;
- iii. An explanation of the labels received on containers acquired at a NIST workplace;
- iv. An explanation of the labeling system employed at a NIST workplace; and
- v. An explanation of the SDSs, including the order of information and how employees and covered associates can obtain and use appropriate hazard information.

(b) Information provided by the OU/division on the hazardous chemicals in the employee's or associate's work area(s), covering the following topics:

- i. Any activities in the work area where hazardous chemicals are present;
- ii. How to obtain access to the Hazardous Chemical Inventory List and SDSs for the hazardous chemicals in the work area.

(c) Training provided by the OU/division on the hazardous chemicals in the employee's or associate's work area(s), covering the following topics:

- i. The physical, health, simple asphyxiation, combustible dust, and pyrophoric gas hazards, as well as the hazards not otherwise classified, of the hazardous chemicals in the work area;

571 ii. Measures employees and covered associates can take to protect themselves from
572 these hazards, including specific procedures implemented to prevent exposure to
573 the hazardous chemicals in the work area, such as appropriate work practices,
574 emergency procedures, and personal protective equipment; and,

575
576 iii. Methods and observations that may be used to detect the presence or release of
577 the hazardous chemicals in the work area.

578
579 Note: Training for a specific work area shall be provided in accordance with the
580 requirements of the OU/division to which the specific work area is assigned.

581
582 (4) All employees and covered associates to whom this suborder applies shall receive the
583 following information whenever a new chemical hazard for which they previously have
584 not been trained is introduced into their work area:

585
586 (a) Information provided by the OU/division, covering the following topics:

587
588 i. Any operations in the work area where the new chemical hazard is present;

589
590 (5) All employees and covered associates to whom this suborder applies shall receive the
591 following training whenever a new chemical hazard for which they previously have not
592 been trained is introduced into their work area:

593
594 (a) Training provided by the OU/division, covering the following topics:

595
596 i. A description of the new chemical hazard;

597
598 ii. Measures employees and covered associates can take to protect themselves from
599 the new chemical hazard in the work area; and

600
601 iii. Methods and observations that may be used to detect the presence or release of
602 the new, chemical hazard in the work area.

603
604 Note: Training for a specific work area shall be provided in accordance with the
605 requirements of the OU/division to which the specific work area is assigned.

606
607 (6) All employees and covered associates to whom this suborder applies shall receive
608 information and training as specified in the OSHA Chemical-Specific Health Standards,
609 when applicable (see Appendix B).

h. Informing Other Employers

(1) The employers of personnel who are not NIST employees or covered associates and may be exposed to hazardous chemicals owned by NIST employees and covered associates under normal conditions of use or in a foreseeable emergency (see definition of “Foreseeable Emergency”) shall be provided with the following upon request:

(a) On-site access to SDSs, either electronically or in hard copy, for the hazardous chemicals to which their personnel may be exposed;

(b) Information on the training provided to their personnel on any precautionary measures that their personnel need to take to protect themselves during the workplace's normal operating conditions and in foreseeable emergencies; and

(c) Copies of this program, including a description of the labeling system used at pertinent NIST workplaces.

7. DEFINITIONS

a. Activity – An experiment, operation, process, or job, often comprising subtasks, conducted to achieve a specific outcome.

b. Article – A manufactured item (e.g., a plastic pipe, silicon wafer) other than a fluid or particle: (i) which is formed to a specific shape or design during manufacture; (ii) which has end use function(s) dependent in whole or in part upon its shape or design during end use; and (iii) which under normal conditions of use does not release more than very small quantities, e.g., minute or trace amounts of a hazardous chemical (as determined in 29 CFR 1910.1200(d)), and does not pose a physical hazard or health risk to individuals.

c. Biohazard – A biological material or agent that presents potential risk to the health of humans or other organisms either directly through infection or indirectly through damage to the environment. Biohazards include, but are not limited to, bacteria; fungi; viruses; parasites; rickettsia; biological toxins; prions; non-human mammalian cell lines and tissues; human specimens such as human blood, serum, plasma, blood products, primary and continuous human cell lines, unfixed human tissues, fecal materials, semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, pericardial fluid, peritoneal fluid, amniotic fluid, saliva, tears, sweat, breast milk, and urine; and recombinant DNA materials such as inserts or vectors that are known to express toxins, oncogenes, and/or virulent factors. Non-toxic proteins and commercially available enzymes, cell culture

medium and supplements, reagents such as monoclonal antibodies, and random DNA base pairs are not considered biohazards.

- d. Biohazardous Material – See definition of biohazard.
- e. Chemical – Any substance or mixture of substances.
- f. Chemical Hazard Classification – To identify the relevant data regarding the hazards of a chemical; review those data to ascertain the hazards associated with the chemical; and decide whether the chemical will be classified as hazardous (see definition “Hazardous Chemical”). In addition, Chemical Hazard Classification for health and physical hazards includes the determination of the degree of hazard, where appropriate, by comparing the data with the HCS criteria for health and physical hazards.
- g. Chemical Hazard Determination – To identify the relevant data regarding the hazards of a chemical; review those data to ascertain the hazards associated with the chemical by comparing the data with the HCS criteria for health and physical hazards; and deciding whether the chemical will be classified as hazardous (see definition “Hazardous Chemical”). Chemical Hazard Determination does not include determining the degree of each health and physical hazard.
- h. Chemical Hazard Warning – Any words, pictures, symbols, or combination thereof that appears on a container label, other form of warning (e.g., placard, sign), or SDS which conveys the hazards of a chemical in a container.
- i. Chemical Manufacturer – An employer with a workplace where chemical(s) are produced for use or distribution. Note: Laboratory employers that ship hazardous chemicals are considered to be either a chemical manufacturer or distributor.
- j. Chemical Name – The scientific designation of a chemical in accordance with the nomenclature system developed by the International Union of Pure and Applied Chemistry (IUPAC) or the Chemical Abstracts Service (CAS) rules of nomenclature, or a name that will clearly identify the chemical for the purpose of conducting a hazard classification.
- k. Chemical Owner – A NIST employee or covered associate whose name appears on one or more chemical containers.
- l. Chemical Owner Name – The first name or first initial and last name of the NIST Chemical Owner.

- m. CISPro[®] – A relational database system currently used by NIST for tracking chemical inventory, generating labels, and managing SDSs.
- n. Combustible Dust – A combustible particulate solid that presents a fire or deflagration hazard when suspended in air or some other oxidizing medium over a range of concentrations, regardless of particle size or shape.
- o. Common Name – Any designation or identification such as code name, code number, trade name, brand name or generic name used to identify a chemical other than by its chemical name.
- p. Consumer Product – Any article, or component part thereof, produced or distributed (i) for sale to a consumer for use in or around a permanent or temporary household or residence, a school, in recreation, or otherwise, or (ii) for the personal use, consumption or enjoyment of a consumer in or around a permanent or temporary household or residence, a school, in recreation, or otherwise.
- q. Container – Any bag, barrel, bottle, box, can, cylinder, drum, reaction vessel, storage tank, or the like that contains a hazardous chemical. For purposes of this program, pipes or piping systems, and engines, fuel tanks, or other operating systems in a vehicle, are not considered to be containers.
- r. Distributor – A business, other than a chemical manufacturer or importer, which supplies hazardous chemicals to other distributors or to employers. Note: Laboratory employers that ship hazardous chemicals are considered to be either a chemical manufacturer or distributor.
- s. Document Custodian – An OSHE employee assigned to serve as the point of contact for a specific document and to carry out the responsibilities delineated in the Document and Record Control Program.
- t. Exposure or Exposed – An employee is subjected in the course of employment to a chemical that is a physical or health hazard, and includes potential (e.g. accidental or possible) exposure. "Subjected" in terms of health hazards includes any route of entry (e.g. inhalation, ingestion, skin contact or absorption).
- u. Foreseeable Emergency – Any potential occurrence such as, but not limited to, equipment failure, rupture of containers, or failure of control equipment which could result in an uncontrolled release of a hazardous chemical into the workplace.

- v. Hazard Category – The division of criteria within each hazard class, *e.g.*, oral acute toxicity and flammable liquids include four hazard categories. These categories compare hazard severity within a hazard class and should not be taken as a comparison of hazard categories more generally.
- w. Hazard Class – The nature of the physical or health hazards (*e.g.*, flammable solid, carcinogen, oral acute toxicity).
- x. Hazard Not Otherwise Classified (HNOC) – An adverse physical or health effect identified through evaluation of scientific evidence during the Chemical Hazard Classification or Chemical Hazard Determination process that does not meet the specified criteria for the physical and health hazard classes addressed in 29 CFR 1910.1200. This does not extend coverage to adverse physical and health effects for which there is a hazard class addressed in 29 CFR 1910.1200, but the effect either falls below the cut-off value/concentration limit of the hazard class or is under a GHS hazard category that has not been adopted by OSHA (*e.g.*, acute toxicity Category 5).
- y. Hazard Statement – A statement assigned to a hazard class and category that describes the nature of the hazard(s) of a chemical, including, where appropriate, the degree of hazard.
- z. Hazardous Chemical – Any chemical which is classified as a physical hazard or a health hazard, a simple asphyxiant, combustible dust, pyrophoric gas, or hazard not otherwise in accordance with 29 CFR 1910.1200.
- aa. Health Hazard – A chemical which is classified as posing one of the following hazardous effects: acute toxicity (any route of exposure); skin corrosion or irritation; serious eye damage or eye irritation; respiratory or skin sensitization; germ cell mutagenicity; carcinogenicity; reproductive toxicity; specific target organ toxicity (single or repeated exposure); or aspiration hazard. The criteria for determining whether a chemical is classified as a health hazard are detailed in 29 CFR 1910.1200-Appendix A.
- bb. Immediate Use – The hazardous chemical will be under the control of and used only by the person who transfers it from a labeled container and only within the work shift in which it is transferred.
- cc. Importer – The first business with employees within the Customs Territory of the United States which receives hazardous chemicals produced in other countries for the purpose of supplying them to distributors or employers within the United States.

- dd. Label – An appropriate group of written, printed or graphic information elements concerning a hazardous chemical that is affixed to, printed on, or attached to the immediate container of a hazardous chemical, or to the outside packaging.
- ee. Label Elements – The specified pictogram, hazard statement, signal word and precautionary statement for each hazard class and category, as specified in 29 CFR 1910.1200-Appendix C.
- ff. Laboratory – For the purposes of this program, a work area where the “Laboratory Use” (see definition of “Laboratory Use”) of hazardous chemicals occurs. It is a workplace where relatively small quantities of hazardous chemicals are used on a non-production basis.
- gg. Laboratory Scale – For the purposes of this program, scale of work in which the procedures/containers used for reactions, transfers, and other handling of chemicals are designed to be easily and safely carried out/manipulated by one person. "Laboratory Scale" excludes work whose purpose is to produce commercial quantities of materials.
- hh. Laboratory Use – For the purposes of this program, use of hazardous chemicals in which all of the following conditions are met:
- (1) Chemical manipulations are carried out on a "Laboratory Scale" (see definition of “Laboratory Scale”);
 - (2) Multiple chemical procedures or chemicals are used²⁴;
 - (3) The procedures involved are not part of a production process, nor in any way simulate a production process; and
 - (4) "Protective Laboratory Practices and Equipment" (see definition of “Protective Laboratory Practices and Equipment”) are available and in common use to minimize the potential for employee exposure to hazardous chemicals.
- ii. LC RAM (Limited Control RAM) – RAM that is:
- (1) Byproduct material exempted under 10 CFR 30;
 - (2) Unimportant quantities of source material as per 10 CFR 40.13;

²⁴ [OSHA LOI # 20164](#) describes that “Multiple chemical procedures or chemicals are used” means “using chemicals in laboratory procedures”, which includes scenarios involving a single chemical or single procedure.

(3) RAM such as that described in 10 CFR 31.8, 10 CFR 40.22, and 10 CFR 70.19 that is not part of a GL device;

(4) Incidentally-Activated RAM; or

(5) Any other RAM determined by the RSO to warrant some degree of control for RSP purposes.

jj. Mixture – A combination or a solution composed of two or more substances in which they do not react.

kk. NIST Visitor – Any individual at a NIST workplace who is not a NIST employee or associate.

ll. NIST Workplace – An establishment at one geographical location containing one or more “work areas” and at which NIST employees and covered associates conduct work (see definition of “Work Area”). NIST workplaces include, but are not limited to, NIST Gaithersburg, NIST Boulder, and NIST joint institutes.

mm. Non-Hazardous Chemical – For the purposes of this program, any chemical that does not meet the definition of “Hazardous Chemical” (see definition “Hazardous Chemical”).

nn. Non-Laboratory Use – For the purposes of this program, use of hazardous chemicals that does not meet the definition of “Laboratory Use” (see definition of “Laboratory Use”).

oo. Organizational Unit (OU)-Assigned Space or Work Area – For the purposes of this program, a space or work area assigned to an OU in the NIST space management system maintained by the Office of Facilities and Property Management or assigned to an OU by another OU on a non-permanent basis (i.e., loaned).

pp. Package – A receptacle and any other components or materials necessary for the receptacle to perform its containment function in conformance with the minimum packing requirements of the U. S. Department of Transportation's Hazardous Materials Regulations (49 CFR Parts 171 through 180).

qq. Physical Hazard – A chemical that is classified as posing one of the following hazardous effects: explosive; flammable (gases, aerosols, liquids, or solids); oxidizer (liquid, solid or gas); self-reactive; pyrophoric (liquid or solid); self-heating; organic peroxide; corrosive to metal; gas under pressure; or in contact with water emits flammable gas. The criteria for

determining whether a chemical is classified as a physical hazard are detailed in 29 CFR 1910.1200-Appendix B.

- rr. Pictogram – A composition that may include a symbol plus other graphic elements, such as a border, background pattern, or color, that is intended to convey specific information about the hazards of a chemical. Eight pictograms are designated under 29 CFR 1910.1200 for application to a hazard category.
- ss. Precautionary Statement – A phrase that describes recommended measures that should be taken to minimize or prevent adverse effects resulting from exposure to a hazardous chemical, or improper storage or handling.
- tt. Produce – To manufacture, process, formulate, blend, extract, generate, emit, package, or repackage.
- uu. Product Identifier – The name or number used for a hazardous chemical on a label or in the SDS. It provides a unique means by which the user can identify the chemical. The product identifier used shall permit cross-references to be made among the list of hazardous chemicals required in the written hazard communication program, the label and the SDS.
- vv. Protective Laboratory Practices and Equipment – Laboratory practices and equipment accepted by laboratory health and safety experts as effective, or that the employer can show to be effective, in minimizing the potential for employee exposure to hazardous chemicals.
- ww. Pyrophoric Gas – A chemical in a gaseous state that will ignite spontaneously in air at a temperature of 130 degrees F (54.4 degrees C) or below.
- xx. RAM (Radioactive Material) – Material permitted at NIST Gaithersburg under SNM-362, a GL, or as LC RAM.
- yy. Responsible Party – Someone who can provide additional information on the hazardous chemical and appropriate emergency procedures, if necessary.
- zz. Safety Data Sheet (SDS) – Written or printed material concerning a hazardous chemical that is prepared in accordance with paragraph (g) of 29 CFR 1910.1200.
- aaa. Shipped Container – Any container that leaves the NIST workplace.
- bbb. Signal Word – A word used to indicate the relative level of severity of hazard and alert the reader to a potential hazard on the label. The signal words used in 29 CFR 1910.1200 and

this program are "DANGER" and "WARNING." "DANGER" is used for the more severe hazards, while "WARNING" is used for the less severe.

- ccc. Simple Asphyxiant – A substance or mixture that displaces oxygen in the ambient atmosphere, and can thus cause oxygen deprivation in those who are exposed, leading to unconsciousness and death.
- ddd. SNM (Special Nuclear Material) –
- (1) Plutonium, uranium-233, uranium enriched in the isotope 233 or in the isotope 235, and any other material that the NRC determines to be SNM, but not including source material; or
 - (2) Any material artificially enriched by any of the foregoing, but not including source material.
- eee. SNM-362 – A NRC license authorizing acquisition, use, transfer, and disposal of any chemical or physical form of the byproduct material specified in the license, but not exceeding quantities specified in the license, for purposes authorized by the license.
- fff. SNM-362 RAM – Byproduct material, source material, and SNM that is acquired, possessed, used, transferred, or disposed of under SNM-362.
- ggg. Specific Chemical Identity – The chemical name, Chemical Abstracts (CAS) Registry Number, or any other information that reveals the precise chemical designation of the substance.
- hhh. Stationary Process Container – A chemical process container that is not capable of being moved.
- iii. Substance – Chemical elements and their compounds in the natural state or obtained by any production process, including any additive necessary to preserve the stability of the product and any impurities deriving from the process used, but excluding any solvent which may be separated without affecting the stability of the substance or changing its composition.
- jjj. Use – To package, handle, react, emit, extract, generate as a byproduct, or transfer.
- kkk. Work Area – A defined space in a workplace where hazardous chemicals are produced or used to which there is a reasonable likelihood that workers present in the space could be exposed.

926 III. Workplace – See definition “NIST Workplace”.
927
928

929 **8. ACRONYMS**

930 a. CFR – Code of Federal Regulations
931

932 b. HCS – OSHA 29 CFR 1910.1200, *Hazard Communication in General Industry*
933

934 c. NIST – National Institute of Standards and Technology
935

936 d. ORM – Office of Reference Materials
937

938 e. OSH – Occupational Safety and Health
939

940 f. OSHA – Occupational Safety and Health Administration
941

942 g. OSHE – Office of Safety, Health, and Environment
943

944 h. OU – Organizational Unit
945

946 i. SDS – Safety Data Sheet
947
948

949 **9. RESPONSIBILITIES**

950 a. OU Directors²⁵ are responsible for:
951

952 (1) Establishing policies and procedures, as needed, for the requirements of this program to
953 be met as it applies to their employees and covered associates and to hazardous chemicals
954 in their OU-assigned space and ensuring that those policies and procedures are
955 implemented; and
956

957 (2) Ensuring subordinate managers have the authority, resources, and training needed to
958 implement OU-established policies and procedures.
959

²⁵ For each of the laboratory divisions in Boulder, Colorado, the NIST Boulder Labs Director and the Laboratory Director for the division in question each have these responsibilities. They should work together to coordinate their respective policies and procedures to the maximum extent possible to minimize any additional and undue burden on the division, which must otherwise follow two different sets of policies and procedures.

- b. Division Chiefs (or Equivalents)²⁶ are responsible for:
- (1) Implementing this program as it applies to activities involving their personnel and space in accordance with any applicable OU-established policies and procedures.
- c. Organizational Unit (OU)/Division Safety Personnel are responsible for:
- (1) Participating in the implementation of this program in accordance with any applicable OU/division-established policies and procedures.
- d. Chemical Owners²⁷ are responsible for:
- (1) Ensuring that Chemical Hazard Classifications and Chemical Hazard Determinations have been performed in accordance with the requirements of this suborder for the chemicals they own;
 - (2) Ensuring that labels and other forms of warning have been provided according to the requirements of this suborder for chemicals they own;
 - (3) Taking appropriate action when notified by a user of a chemical container they own that the label on that container is illegible or contains information that is not current;
 - (4) Ensuring that SDSs have been obtained, produced, maintained, and provided according to the requirements of this suborder for chemicals they own;
 - (5) Ensuring that the Hazardous Chemical Inventory List has been maintained according to the requirements of this suborder for the chemicals they own;
 - (6) Ensuring that other employees and covered associates in the same work area will be informed when a new chemical hazard is to be introduced into the work area²⁸; and
 - (7) Carrying out other duties as assigned for the chemicals they own in accordance with any applicable OU/division-established policies and procedures.

²⁶ Some NIST OUs do not have Division Chiefs; these OUs shall designate other individuals to carry out these responsibilities.

²⁷ These responsibilities are those pertinent to this suborder only. Chemical Owners have other responsibilities described in other NIST OSH suborders, including NIST S 7101.60: *Chemical Management (Chemical Hygiene Plan)* and NIST S 7301.4, *Hazardous Waste Accumulation*.

²⁸ Employees and covered associates who become aware of a new, chemical hazard in their work area shall inform their line management of the new, chemical hazard so that line management can ensure that the training requirements of this suborder are met.

- 993 e. Employees and Covered Associates are responsible for:
- 994
- 995 (1) Completing the training required by this program and their OUs/divisions and working in
- 996 accordance with that training;
- 997
- 998 (2) Requesting additional training as needed or as conditions change;
- 999
- 1000 (3) Knowing the requirements of this suborder;
- 1001
- 1002 (4) Knowing the chemical hazards in the specific work area;
- 1003
- 1004 (5) Ensuring that routine and non-routine activities will be performed according to the
- 1005 requirements of this suborder and any other applicable suborder;
- 1006
- 1007 (6) Knowing the method for obtaining access to the Hazardous Chemical Inventory List and
- 1008 SDSs for the hazardous chemicals in the specific work area;
- 1009
- 1010 (7) Reading chemical container labels, other forms of warning, and SDSs prior to using
- 1011 hazardous chemicals for the first time and as needed thereafter;
- 1012
- 1013 (8) Notifying the Chemical Owner if they identify a label on a chemical container that is
- 1014 illegible or contains information that is not current; and
- 1015
- 1016 (9) Contacting line managers, Organizational Unit (OU)/Divisional Safety Personnel, and/or
- 1017 the OSH program manager for this program regarding any questions related to the hazard
- 1018 communication training and information provided on chemical container labels, other
- 1019 forms of warning, and SDSs.
- 1020
- 1021 f. OSH Program Manager for this program is responsible for:
- 1022
- 1023 (1) Providing NIST employees and covered associates with straightforward interpretations
- 1024 and explanations of how relevant regulations, codes, and standards in this program area
- 1025 apply in the NIST environment; and
- 1026
- 1027 (2) Making this suborder available upon request and in accordance with the requirements of
- 1028 29 CFR 1910.1020(e).
- 1029
- 1030
- 1031
- 1032

1033 **10. AUTHORITIES**

1034 There are no authorities specific to this suborder alone. For authorities applicable to all NIST OSH
1035 suborders, see section 9 of [NIST O 710.01](#).

1036

1037

1038 **11. DIRECTIVE OWNER**

1039 Chief Safety Officer

1040

1041

1042 **12. APPENDICES**

1043 a. Revision History

1044

1045 b. Chemicals Regulated in OSHA Chemical-Specific Health Standards

1046
1047

Appendix A. Revision History

Revision No.	Approval Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	04/29/14	05/21/14	04/01/15	<ul style="list-style-type: none">• None – Initial document
1	02/08/15	02/08/15	10/01/16	<ul style="list-style-type: none">• Minor revision to “Hazardous Chemical” definition. Minor revision for formatting.• Addition of footnote and definitions pertaining to inventory requirements for Biohazardous Materials, LC-RAM, and SNM-362 RAM.• Minor revision to Section 6g to differentiate between information requirements and training requirements.• Added text to Section 9d to assign Chemical Owners the responsibility of ensuring that Chemical Hazard Classifications and Chemical Hazard Determinations have been performed in accordance with the requirements of the suborder.• Minor revision to Section 6d to clarify Hazardous Chemical Inventory Lists requirements and to include a footnote pertaining to SRMs.• Revised footnote 2 and changed “associate” to “covered associate” throughout suborder to update text with current NIST definitions of “associate” and “covered”.

1048

Appendix B. Chemicals Regulated in OSHA Chemical-Specific Health Standards

This appendix provides basic information regarding whether a chemical is within the scope and application of the OSHA Chemical-Specific Health Standards. The OSHA Chemical-Specific Health Standards (29 CFR 1910.1001 - 29 CFR 1910.1052) provide numerous requirements (e.g., hazard communication, information and training, permissible exposure limits, and exposure monitoring/medical surveillance) for specific chemicals. The application and therefore applicable requirements of the OSHA Chemical-Specific Health Standards are determined by criteria such as chemical concentration, physical form, and use. The OSHA Chemical-Specific Health Standards should be consulted for detailed information regarding the applicable requirements. The OSH Safety Program Manager for this program or another OSHE staff member will provide assistance upon request.

- a. When the use of a chemical at a NIST workplace meets the definition of “Laboratory Use” and is within the scope and application of an OSHA Chemical-Specific Health Standard, OSHA 29 CFR 1910.1450, *Occupational Exposure to Hazardous Chemicals in Laboratories* supercedes the requirements of the particular OSHA Chemical-Specific Health Standard, except as follows:

- (1) 1910.1450(a)(2)(i) For any OSHA health standard, only the requirement to limit employee exposure to the specific permissible exposure limit shall apply for laboratories, unless that particular standard states otherwise or unless the conditions of 1910.1450(a)(2)(iii) apply (see below);
- (2) 1910.1450(a)(2)(ii) Prohibition of eye and skin contact where specified by any OSHA health standard shall be observed;
- (3) 1910.1450(a)(2)(iii) Where the action level (or in the absence of an action level, the permissible exposure limit) is routinely exceeded for an OSHA regulated substance with exposure monitoring and medical surveillance requirements of 1910.1450(d) and 1910.1450(g)(1)(ii) shall apply.

Note: The hazard communication requirements of the OSHA Chemical-Specific Health Standards are not applicable to chemical uses that meet the definition of “Laboratory Use”.

- b. When the use of a chemical at a NIST workplace does not meet the definition of “Laboratory Use” and is within the scope and application of an OSHA Chemical-Specific Health Standard, all requirements of the particular OSHA Chemical-Specific Health Standard are applicable, including the hazard communications requirements.

c. Scope and Application of OSHA Chemical-Specific Health Standards:

(1) [29 CFR 1910.1001, *Asbestos*](#)

(a) This section applies to all occupational exposures to asbestos in all industries covered by the Occupational Safety and Health Act, except:

- i. This section does not apply to construction work as defined in 29 CFR 1910.12(b). (Exposure to asbestos in construction work is covered by 29 CFR 1926.1101.); and
- ii. This section does not apply to ship repairing, shipbuilding and shipbreaking employments and related employments as defined in 29 CFR 1915.4. (Exposure to asbestos in these employments is covered by 29 CFR 1915.1001).

(2) [29 CFR 1910.1003, *13 Carcinogens*](#)

(a) This section applies to any area in which the 13 carcinogens addressed by this section are manufactured, processed, repackaged, released, handled, or stored, but shall not apply to transshipment in sealed containers, except for the labeling requirements under paragraphs (e)(2), (3) and (4) of this section. The 13 carcinogens are the following: 4-Nitrobiphenyl, Chemical Abstracts Service Register Number (CAS No.) 92933; alpha-Naphthylamine, CAS No. 134327; methyl chloromethyl ether, CAS No. 107302; 3,3'-Dichlorobenzidine (and its salts) CAS No. 91941; bis-Chloromethyl ether, CAS No. 542881; beta-Naphthylamine, CAS No. 91598; Benzidine, CAS No. 92875; 4-Aminodiphenyl, CAS No. 92671; Ethyleneimine, CAS No. 151564; beta-Propiolactone, CAS No. 57578; 2-Acetylaminofluorene, CAS No. 53963; 4-Dimethylaminoazo-benzene, CAS No. 60117; and N-Nitrosodimethylamine, CAS No. 62759.

(b) This section shall not apply to the following:

- i. Solid or liquid mixtures containing less than 0.1 percent by weight or volume of 4-Nitrobiphenyl; methyl chloromethyl ether; bis-chloromethyl ether; beta-Naphthylamine; benzidine or 4-Aminodiphenyl; and
- ii. Solid or liquid mixtures containing less than 1.0 percent by weight or volume of alpha-Naphthylamine; 3,3'-Dichlorobenzidine (and its salts); Ethyleneimine; beta-Propiolactone; 2-Acetylaminofluorene; 4-Dimethylaminoazobenzene, or N-Nitrosodimethylamine.

(3) [29 CFR 1910.1017, Vinyl Chloride](#)

(a) This section applies to the manufacture, reaction, packaging, repackaging, storage, handling or use of vinyl chloride or polyvinyl chloride, but does not apply to the handling or use of fabricated products made of polyvinyl chloride.

(b) This section applies to the transportation of vinyl chloride or polyvinyl chloride except to the extent that the Department of Transportation may regulate the hazards covered by this section.

(4) [29 CFR 1910.1018, Inorganic Arsenic](#)

(a) This section applies to all occupational exposures to inorganic arsenic except that this section does not apply to employee exposures in agriculture or resulting from pesticide application, the treatment of wood with preservatives or the utilization of arsenically preserved wood.

(5) [29 CFR 1910.1025, Lead](#)

(a) This section applies to all occupational exposure to lead, except:

i. This section does not apply to the construction industry or to agricultural operations covered by 29 CFR Part 1928.

(6) [29 CFR 1910.1026, Chromium \(VI\)](#)

(a) This standard applies to occupational exposures to chromium (VI) in all forms and compounds in general industry, except:

i. Exposures that occur in the application of pesticides regulated by the Environmental Protection Agency or another Federal government agency (e.g., the treatment of wood with preservatives);

ii. Exposures to portland cement; or

iii. Where the employer has objective data demonstrating that a material containing chromium or a specific process, operation, or activity involving chromium cannot release dusts, fumes, or mists of chromium (VI) in concentrations at or above 0.5 $\mu\text{g}/\text{m}^3$ as an 8-hour time-weighted average (TWA) under any expected conditions of use.

(7) [29 CFR 1910.1027, Cadmium](#)

- (a) This standard applies to all occupational exposures to cadmium and cadmium compounds, in all forms, and in all industries covered by the Occupational Safety and Health Act, except the construction-related industries, which are covered under 29 CFR 1926.63.

(8) [29 CFR 1910.1028, Benzene](#)

- (a) This section applies to all occupational exposures to benzene. Chemical Abstracts Service Registry No. 71-43-2, except:

- i. The storage, transportation, distribution, dispensing, sale or use of gasoline, motor fuels, or other fuels containing benzene subsequent to its final discharge from bulk wholesale storage facilities, except that operations where gasoline or motor fuels are dispensed for more than 4 hours per day in an indoor location are covered by this section.
- ii. Loading and unloading operations at bulk wholesale storage facilities which use vapor control systems for all loading and unloading operations, except for the provisions of 29 CFR 1910.1200 as incorporated into this section and the emergency provisions of paragraphs (g) and (i)(4) of this section.
- iii. The storage, transportation, distribution or sale of benzene or liquid mixtures containing more than 0.1 percent benzene in intact containers or in transportation pipelines while sealed in such a manner as to contain benzene vapors or liquid, except for the provisions of 29 CFR 1910.1200 as incorporated into this section and the emergency provisions of paragraphs (g) and (i)(4) of this section.
- iv. Containers and pipelines carrying mixtures with less than 0.1 percent benzene and natural gas processing plants processing gas with less than 0.1 percent benzene.
- v. Work operations where the only exposure to benzene is from liquid mixtures containing 0.5 percent or less of benzene by volume, or the vapors released from such liquids until September 12, 1988; work operations where the only exposure to benzene is from liquid mixtures containing 0.3 percent or less of benzene by volume or the vapors released from such liquids from September 12, 1988, to September 12, 1989; and work operations where the only exposure to benzene is from liquid mixtures containing 0.1 percent or less of benzene by volume or the vapors released from such liquids after September 12, 1989; except that tire

building machine operators using solvents with more than 0.1 percent benzene are covered by paragraph (i) of this section.

vi. Oil and gas drilling, production and servicing operations.

vii. Coke oven batteries.

viii. The cleaning and repair of barges and tankers which have contained benzene are excluded from paragraph (f) methods of compliance, paragraph (e)(1) exposure monitoring-general, and paragraph (e)(6) accuracy of monitoring. Engineering and work practice controls shall be used to keep exposures below 10 ppm unless it is proven to be not feasible.

(9) [29 CFR 1910.1029, Coke Oven Emissions](#)

(a) This section applies to the control of employee exposure to coke oven emissions, except that this section shall not apply to working conditions with regard to which other Federal agencies exercise statutory authority to prescribe or enforce standards affecting occupational safety and health.

(10) [29 CFR 1910.1044, 1,2-Dibromo-3-Chloropropane](#)

(a) This section applies to occupational exposure to 1,2-dibromo-3-chloropropane (DBCP), except:

- i. Exposure to DBCP which results solely from the application and use of DBCP as a pesticide; or
- ii. The storage, transportation, distribution or sale of DBCP in intact containers sealed in such a manner as to prevent exposure to DBCP vapors or liquid, except for the requirements of paragraphs (i), (n) and (o) of this section.

(11) [29 CFR 1910.1045, Acrylonitrile](#)

(a) This section applies to all occupational exposures to acrylonitrile (AN), Chemical Abstracts Service Registry No. 000107131, except:

- i. This section does not apply to exposures which result solely from the processing, use, and handling of the following materials:

- (i) ABS resins, SAN resins, nitrile barrier resins, solid nitrile elastomers, and acrylic and modacrylic fibers, when these listed materials are in the form of finished polymers, and products fabricated from such finished polymers;
- (ii) Materials made from and/or containing AN for which objective data is reasonably relied upon to demonstrate that the material is not capable of releasing AN in airborne concentrations in excess of 1 ppm as an eight (8)-hour time-weighted average, under the expected conditions of processing, use, and handling which will cause the greatest possible release; and
- (iii) Solid materials made from and/or containing AN, which will not be heated above 170 deg. F during handling, use, or processing.

(12) [29 CFR 1910.1047, Ethylene Oxide](#)

- (a) This section applies to all occupational exposures to ethylene oxide (EtO), Chemical Abstracts Service Registry No. 75-21-8, except:
- i. This section does not apply to the processing, use, or handling of products containing EtO where objective data are reasonably relied upon that demonstrate that the product is not capable of releasing EtO in airborne concentrations at or above the action level under the expected conditions of processing, use, or handling that will cause the greatest possible release.

(13) [29 CFR 1910.1048, Formaldehyde](#)

- (a) This standard applies to all occupational exposures to formaldehyde, i.e. from formaldehyde gas, its solutions, and materials that release formaldehyde.

(14) [29 CFR 1910.1050, Methylenedianiline](#)

- (a) This section applies to all occupational exposures to MDA, Chemical Abstracts Service Registry No. 101-77-9, except:
- i. Except as provided in paragraphs (a)(8) and (e)(5) of this section, this section does not apply to the processing, use, and handling of products containing MDA where initial monitoring indicates that the product is not capable of releasing MDA in excess of the action level under the expected conditions of processing, use, and handling which will cause the greatest possible release; and where no "dermal exposure to MDA" can occur.

- 1289 ii. Except as provided in paragraph (a)(8) of this section, this section does not apply
1290 to the processing, use, and handling of products containing MDA where objective
1291 data are reasonably relied upon which demonstrate the product is not capable of
1292 releasing MDA under the expected conditions of processing, use, and handling
1293 which will cause the greatest possible release; and where no "dermal exposure to
1294 MDA" can occur.
1295
- 1296 iii. This section does not apply to the storage, transportation, distribution or sale of
1297 MDA in intact containers sealed in such a manner as to contain the MDA dusts,
1298 vapors, or liquids, except for the provisions of 29 CFR 1910.1200 and paragraph
1299 (d) of this section.
1300
- 1301 iv. This section does not apply to the construction industry as defined in 29 CFR
1302 1910.12(b). (Exposure to MDA in the construction industry is covered by 29 CFR
1303 1926.60).
1304
- 1305 v. Except as provided in paragraph (a)(8) of this section, this section does not apply
1306 to materials in any form which contain less than 0.1 percent MDA by weight or
1307 volume.
1308
- 1309 vi. Except as provided in paragraph (a)(8) of this section, this section does not apply
1310 to "finished articles containing MDA."
1311

1312 (15) [29 CFR 1910.1051, 1,3-Butadiene](#)
1313

- 1314 (a) This section applies to all occupational exposures to 1,3-Butadiene (BD), Chemical
1315 Abstracts Service Registry No. 106-99-0, except as provided in paragraph (a)(2) of
1316 this section.
1317

1318 (16) [29 CFR 1910.1052, Methylene Chloride](#)
1319

- 1320 (a) This section applies to all occupational exposures to methylene chloride (MC),
1321 Chemical Abstracts Service Registry Number 75-09-2, in general industry,
1322 construction and shipyard employment.

COMPRESSED GAS SAFETY

NIST S 7101.61

Document Approval Date:¹ 05/27/2015

Effective Date: 04/01/2016

1. PURPOSE

The purpose of this program is to establish requirements to minimize the potential hazards associated with compressed gases in cylinders, vessels, and systems.

2. BACKGROUND

- a. [NIST P 7100.00](#) articulates NIST's commitment to making occupational safety and health an integral core value and vital part of the NIST culture, in part by complying with applicable laws, regulations, and other promulgated safety and health requirements.
- b. The content of this suborder was derived primarily from applicable Compressed Gas Association (GGA P-1) and National Fire Protection Association (NFPA) Codes/Standards (NFPA 45, NFPA 55, and NFPA 704). The hazard definitions and numeric ratings in this suborder are based on NFPA definitions. These are similar to the definitions published in the 1994 version of Occupational Safety and Health Administration (OSHA) standard 29 CFR 1910.1200 – *Hazard Communication*, but they may differ from the definitions published in the 2012 version.
- c. Compressed gases are subject to the requirements of [NIST S 7101.59: Chemical Hazard Communication](#) and [NIST S 7101.60: Chemical Management](#).
- d. This suborder supersedes the NIST *Health and Safety Instruction No. 5 – Compressed Gas Cylinders*.

3. APPLICABILITY

- a. The provisions of this suborder apply to all NIST activities involving:
 - (1) The use of commercially-available compressed gas cylinders, including lecture bottles;
 - (2) Conventional facility and plant pressure vessels and systems; and

¹ The revision history for this document can be found in Appendix A.

(3) Commercially available-pressure vessels and systems.

- b. The provisions of this suborder apply to specialized laboratory pressure vessels and systems to the maximum extent feasible. When not feasible, the provisions in Section 6d of this suborder apply.

4. REFERENCES²

- a. Compressed Gas Association (CGA) Pamphlet C-6, Standards for Visual Inspection of Steel Compressed Gas Cylinders.
- b. CGA Pamphlet C-7, Guide to Preparation of Precautionary Labeling and Marking of Compressed Gas Containers.
- c. CGA Pamphlet C-8, Standard for Requalification of DOT-3HT, CTC-3HT, and TC-3HTM Seamless Steel Cylinders.
- d. CGA Pamphlet P-1, Safe Handling of Compressed Gases in Containers.
- e. CGA Pamphlet P-19, Recommended Hazard Ratings for Compressed Gases.
- f. CGA Pamphlet P-20, Standard for Classification of Toxic Gas Mixtures.
- g. CGA Pamphlet S-1.1, Pressure Relief Device Standards Part 1 – Cylinders for Compressed Gases.
- h. CGA Pamphlet S-1.2, Pressure Relief Device Standards Part 2 – Portable Containers for Compressed Gases.
- i. Industrial Ventilation, a Manual of Recommended Practice, American Conference of Governmental Industrial Hygienists (ACGIH).
- j. International Organization for Standardization (ISO) Standard 10156, Gas Cylinders – Gases and Gas Mixtures – Determination of Fire Potential and Oxidizing Ability
- k. ISO 10298, Determination of Toxicity of a Gas or Gas Mixture.
- l. NFPA 45, Fire Protection for Laboratories Using Chemicals.

² Where no date is specified, the most recent version applies.

- m. NFPA 50A, Gaseous Hydrogen Systems at Consumer Sites.
- n. NFPA 51, Design and Installation of Oxygen-Fuel Gas Systems for Welding, Cutting, and Allied Processes.
- o. NFPA 51B, Cutting and Welding Processes.
- p. NFPA 55, Compressed and Liquefied Gases in Portable Containers.
- q. NFPA 72, Installation, Maintenance, and Use of Protective Signaling Systems.
- r. NFPA 704, Identification of the Fire Hazards of Materials.
- s. Odor Thresholds for Chemicals with Established Occupational Health Standards, American Industrial Hygiene Association.
- t. OSHA Standard 29 CFR §1910.101, Compressed Gases (general requirements).
- u. Pocket Guide to Chemical Hazards, DHHS (NIOSH), Pub. No. 90-117, National Institute of Occupational Safety and Health LBNL/PUB-3122, Maintenance Program Guidelines for Programmatic Equipment.
- v. Threshold Limit Values for Chemical Substances and Physical Agents, ACGIH.

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. [NIST S 7101.59: Chemical Hazard Communication](#)
- b. [NIST S 7101.60: Chemical Management](#)
- c. [NIST S 7101.20: Hazard Signage](#)
- d. [NIST S 7101.21: Personal Protective Equipment \(PPE\)](#)
- e. [NIST S 7101.58: Respiratory Protection](#)
- f. [NIST S 7101.23: Safety Education and Training](#)

6. REQUIREMENTS

a. General Requirements for the Use of Compressed Gases³

(1) Room Signage where Highly Toxic Gases are Present

- (a) All entrances to areas containing cylinders, vessels, or systems containing highly toxic gases or gases with an NFPA 704 health hazard rating of 4 shall be marked with a “DANGER” sign in accordance with NIST S 7101.20: Hazard Signage. See examples in Figure 1.

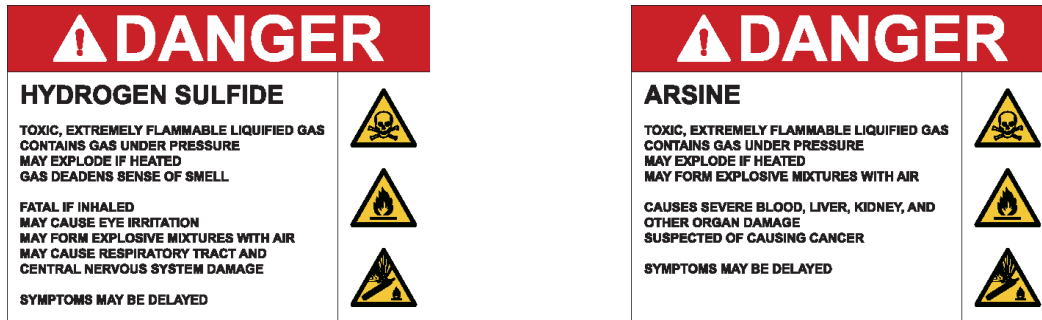


Figure 1: Specific Hazard Signs for Areas Containing Highly Toxic Gases

(2) Room Signage where Compressed Gases are Present

- (a) If smoking is not already prohibited in and near areas containing compressed gases, signs shall be posted in such areas stating that smoking is prohibited within 25 ft (7.6 m) of the storage or use area perimeter.⁴

(3) Ventilation of Compressed Gases

- (a) If compressed gases are introduced into laboratory fume hoods, steps must be taken to ensure that there is no backflow from the fume hood into the surrounding space.
- (b) Local and general exhaust systems used to exhaust hazardous gases shall be constructed of materials that are compatible with the gases to be exhausted.
- (c) Incompatible gases shall be exhausted using separate ventilation systems.

³ Apart from hazard signage, consideration of the chemical hazards associated with the use of specific gases is covered separately in NIST S 7101.60: Chemical Management.

⁴ Smoking is prohibited in NIST buildings and within 25 feet of building entrances and air intakes.

(d) Ventilation systems that will handle flammable gases at concentrations of 10 percent of their Lower Explosive Limit or greater must be explosion-proof and have non-sparking exhaust fans.

(e) Vacuum pumps, high-pressure systems, and pressure-relief devices protecting equipment to be attached to compressed gas cylinders, vessels, or systems containing flammable, toxic, or otherwise hazardous gases should be vented directly outdoors or through an exhaust hood discharging away from windows and doors, and no less than 50 feet (15 m) from intakes of air-handling systems, air-conditioning equipment, and air compressors. If these requirements cannot be met, or their intent can be met using a different approach, the applicable hazard review must identify alternative controls that provide an equivalent level of safety.

(4) Gas Detection Systems for Toxic and Highly Toxic Compressed Gases

(a) A continuous, gas-detection system shall be provided for the indoor storage or use of all toxic or highly toxic compressed gases in cylinders, vessels, or systems, except for toxic gases that have physiological warning properties at a level below the OSHA Permissible Exposure Limit (PEL) or ACGIH Threshold Limit Value (TLV), whichever is lower.⁵

i. A continuous gas detection system may also be appropriate for other hazardous gases, including flammables, pyrophorics, oxidizers, and corrosives, particularly in cases where there are special hazards (for example, as in the case of continuous operations that are unattended). This shall be decided on a case-by-case basis.

(b) The gas-detection system shall detect the presence of gas at or below the ACGIH TLV, OSHA PEL, or ceiling limit of the gas, whichever is lowest, at all of the following locations:

- i. In the room or indoor area in which the gas is used (the point of use);
- ii. At the location of the source container, cylinder, or tank used for delivery of the gas to the point of use;
- iii. In the room or area in which the gas is stored; and

⁵ Contact OSHE at x5375, Option 3 to determine if this requirement applies to a specific compressed gas.

- 184 iv. At the point of discharge of the exhaust system from gas cabinets, exhausted
185 enclosures, and gas rooms, if the point of discharge is not outside the building.
186 (c) The gas detection system shall detect the presence of the gas at not less than one-half
187 of the Immediately Dangerous to Life and Health (IDLH) level at the discharge from
188 any exhaust or waste gas treatment system that is present.
189
190 (d) The gas-detection system shall initiate a local alarm that is both audible and visible.
191
192 (e) All personnel who may be in the area of a local alarm shall be trained in the
193 recognition of the alarms and in the appropriate response in the case of an alarm.
194
195 (f) Gas detection systems shall be required to transmit a signal to a constantly attended
196 monitoring station for any location that contains two or more compressed gas
197 cylinders of toxic or highly toxic gas. The attending organization shall develop
198 response protocols for each different alarm.
199
200 (g) Activation of the gas detection system at a location where compressed gas is hooked
201 up to a system shall automatically shut off the flow of the compressed gas related to
202 the system being monitored.
203
204 i. An automatic shutdown shall not be required for chemical reactors used to
205 produce toxic or highly toxic gases when those reactors are operated at
206 pressures less than 103.4 kPa (15 psig), constantly attended, and have readily
207 accessible, emergency-shutoff valves.
208

209 (5) Personal Protective Equipment
210

- 211 (a) Personal protective equipment (PPE), including respiratory protection as applicable,
212 shall be used when working with compressed gases, as required by the applicable
213 hazard review.⁶
214

215 (6) Eyewashes and Showers
216

- 217 (a) An eyewash station and safety shower shall be provided in each area where corrosive
218 gases are used.
219

220 b. Compressed Gas Cylinders
221

222 (1) Purchasing Compressed Gas Cylinders
223

⁶ The MSDS/SDS for the chemical product will provide guidance on appropriate PPE. The NIOSH Pocket Guide to Chemical Hazards provides guidance on the selection of proper respiratory protection.

- (a) The smallest volumes and numbers of compressed gas cylinders needed to conduct the work effectively shall be purchased.
- (b) Returnable lecture bottles should be purchased whenever possible.

(2) Point-of-Delivery Inspection of Compressed Gas Cylinders

Employees and associates who receive compressed gas cylinders from outside vendors shall conduct point-of-delivery inspections of the cylinders in accordance with the following considerations.⁷ Employees and associates who receive compressed gas cylinders from other individuals within NIST are encouraged to conduct such inspections. Any cylinder not meeting these considerations should not be accepted.⁸

(a) Labeling Requirements

- i. It shall be verified that the compressed gas cylinder is labeled and that the label contains the following information:
 - (i) Product identifier; and
 - (ii) Words, pictures, symbols, or combination thereof, which provide at least general information regarding the hazards of the compressed gas, and which, in conjunction with the other information immediately available to employees and associates under [NIST S 7101.59: Chemical Hazard Communication](#), will provide employees and associates with the specific information regarding the physical and health hazards of the compressed gas.

(b) Visual Inspection

- i. It shall be verified that the compressed gas cylinder is free of visible signs of damage, *e.g.*, cuts, digs, gouges, dents, bulging, corrosion, *etc.*

(c) Leak Testing

- i. It is recommended that compressed gas cylinders containing toxic, highly toxic, corrosive, or flammable gases are leak tested using a hand-held direct-reading thermal conductivity meter (preferred method) or a liquid soap solution or commercially available liquid leak-detection solution. If the

⁷ For the purposes of this section, the Storeroom, Logistics Group, Facilities Services Division, Office of Facilities and Property Management in Gaithersburg (hereafter referred to as “Storeroom”) is not considered an external vendor.

⁸ If a cylinder not meeting these considerations has been accepted, contact OSHE at x5375, Option 3.

cylinder cap does not have openings in it, it must be removed before performing the leak test.

(d) Valid Hydrostatic or Ultrasonic Test Date⁹

- i. It shall be verified that the compressed gas cylinder has a valid hydrostatic or ultrasonic test date clearly indicated on the cylinder, typically stamped near the shoulder or into the valve guard ring welded to the cylinder. This testing is performed by the vendor or supplier prior to refilling a cylinder.¹⁰

- (i) Most cylinders require a hydrostatic or ultrasonic test every 5 years.

- (ii) Certain steel cylinders require testing only once every 10 years. These can be recognized by the five-pointed star stamped after the test date.

(3) Transport of Compressed Gas Cylinders

- (a) Gas cylinders shall not be dragged, rolled on their sides, slid, or allowed to strike each other forcefully. Cylinders may be moved short distances (5-10 feet) by rolling them on their bottom edges.

- (b) When lifting a cylinder with a crane, hoist, or derrick, an appropriate lifting device, such as a cradle or net, shall be used. Cylinders shall not be lifted with magnets or slings.

- (c) Cylinders must never be lifted by their valve caps.

- (d) Cylinders transported by truck shall be fastened securely so that they will not fall or strike each other.

- (e) Once delivered to the user, cylinders shall only be transported in a cart or vehicle equipped to secure the cylinder in place.

- i. Such carts or vehicles shall be inspected for defects prior to use.

- ii. Cylinders weighing 11 Kg (25 lb) or less may be hand-carried.

- (f) If a cylinder is to be transported in an elevator, the elevator should be unoccupied, and a sign stating “Gas Cylinder in Transit, Do Not Ride”, or equivalent, should be

⁹ Contact OSHE at x5375, Option 3, with questions or concerns.

¹⁰ A cylinder may remain onsite, either in use or in storage, beyond its retest date. Retesting is only required when a cylinder is refilled and then transported in public. Retesting is also appropriate any time a cylinder had been damaged or potentially weakened, such as by being in a fire. [See DOT regulation 49 CFR 180.205(c)].

attached to the gas cylinder cart or the interior of the elevator. An example is shown in Figure 2. Once the gas cylinder has been placed in the elevator and the desired floor selected, the gas cylinder should be met at the selected floor.

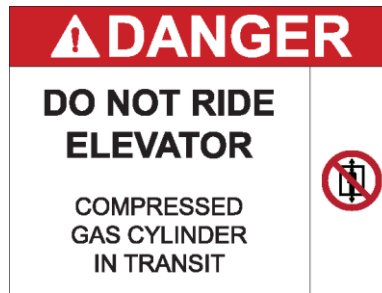


Figure 2: Sign for Transporting Compressed Gas Cylinder in Elevator

- i. Special care should be taken in moving compressed gas cylinders onto and off elevators with regard to both the elevator threshold and the opening and closing of the elevator doors.
 - ii. No one not actually engaged in transporting a compressed gas cylinder on an elevator shall be permitted in the elevator while a cylinder is in transit.
- (g) Cylinders shall only be moved or transported with the regulator removed and the valve protection cap properly secured.

(4) Storage of Compressed Gas Cylinders

- (a) Gas cylinders shall be stored only in indoor and outdoor storage areas that have been determined by a hazard review to meet the requirements of applicable regulations, codes, and standards, especially NFPA 45 and 55.¹¹
 - i. Gas cylinders shall not be stored in laboratories [see Section 6b(5)(c), Maximum Number of Cylinders in Use].¹²
- (b) Gas cylinders shall be stored in such areas in accordance with the requirements of applicable regulations, codes, and standards, especially NFPA 45 and 55..

¹¹ For assistance in establishing new indoor or outdoor storage areas, or of modifying existing storage areas, contact OSHE at x5375, Option 3.

¹² Exceptions to this requirement are possible under certain circumstances. A request for an exception must be submitted to OSHE by a Division Chief (or equivalent) detailing the programmatic need for the exception. OSHE will evaluate the request from a safety and regulatory compliance standpoint and either approve or disapprove it. OSHE will document its evaluation and provide it to the requesting Division Chief. If the request is approved, OSHE's evaluation must be appended to appropriate hazard review(s).

(c) Cylinders Stored in Building Loading Docks in Gaithersburg¹³

- i. Cylinders of normally-stocked gases may be stored in building loading docks for no more than 30 days.
- ii. Cylinders of non-stocked (special order) gases may be stored in building loading docks for no more than 90 days.

(5) Handling and Use of Compressed Gas Cylinders

(a) General Requirements

- i. Cylinders shall be secured at all times to prevent them from falling or being knocked over by securing them to a gas cylinder cart, framework, or fixed object by use of a restraint. Restraints shall be used in such a way that they secure each cylinder individually.¹⁴
 - (i) Restraints designed for the purpose of restraining cylinders should be used.
 - (ii) In locations with large numbers of compressed gas cylinders, nesting using a contiguous 3-point contact system may be utilized. For more information, refer to the definition of "nesting" in Section 7 and Appendix A of CGA P-1.
- ii. Compressed gas cylinders, containers, and tanks shall not be placed where they could become a part of an electrical circuit.
- iii. Compressed gas cylinders containing toxic, highly toxic, corrosive, or flammable gases should be leak tested before being put into service using a hand-held direct-reading thermal conductivity meter (preferred method) or a liquid soap solution or commercially available liquid leak-detection solution. If the cylinder cap does not have openings in it, it must be removed before performing the leak test.

¹³ Exceptions to these requirements in this subsection are possible under certain circumstances. The process for obtaining such an exception is the same as that outlined in the previous footnote except that the Storeroom in Gaithersburg and the OU responsible for managing the loading-dock storage area [see Section 9a(2)] will be included in the safety evaluation of the request.

¹⁴ The best practice for larger cylinders (e.g., 55 inches tall) is to apply one restraint one third of the way up the cylinder and a second restraint two thirds of the way up the cylinder. If only one restraint is available, it should be applied between one half and two thirds of the way up the cylinder.

- iv. Static producing equipment located in flammable gas areas shall be grounded.
- v. Heating, where provided, shall be by indirect means. Equipment used for heating applications in rooms or areas where flammable gases are stored or used shall be listed and labeled for use in hazardous environments established by the gases present and shall be installed in accordance with the conditions of the listing and the manufacturer's installation instructions.
- vi. When not in service, regulators shall be removed and valve protection caps that are not integrated into the cylinder design (and hence technically never removed) properly secured.
- vii. Cylinders, even when partially empty, shall never be heated by any device that could raise the surface temperature of the cylinder to above 52° C (125° F).
- viii. Cylinders should not be emptied to pressures lower than 172 kPa (25 psig) when such pressures could result in contaminants back-flowing into the cylinders and carrying over to when the cylinders are refilled and reused.
- ix. Refilling or transfilling of cylinders shall be performed only by personnel who:
 - (i) Are properly trained and/or qualified to refill or transfill cylinders;
 - (ii) Have the proper equipment to refill or transfill cylinders;
 - (iii) Have approved hazard reviews and written operating procedures for refilling or transfilling cylinders; and
 - (iv) Are familiar with the precautions necessary to avoid the hazards of the product being handled.
- x. If a cylinder is connected to a closed system where there is a possibility of flow reversal, the cylinder shall be shut off and removed from the system while the pressure remaining in the cylinder is still greater than the pressure in the closed system.

(b) Valves and Regulators

- i. Cylinder pressure shall be reduced through a regulator mounted to the cylinder-valve outlet or through a manifold.

- 407 ii. The cylinder valve shall be closed as soon as the necessary amount of gas has
408 been released. The cylinder valve shall never be left open when the
409 equipment is not in use, including when the cylinder is empty.
410
- 411 iii. The cylinder valve, not the regulator, shall be used for turning gas off when
412 the cylinder is not in use.
413
- 414 iv. Only CGA standard combinations of valves and fittings, as specified in CGA
415 Standard V-1, shall be used.
416
- 417 v. Cylinders that are opened with a valve spindle or stem instead of a hand-
418 wheel shall have a spindle key on the spindle while the cylinder is in service.
419
- 420 vi. If tools are required to open cylinder caps or valves, only wrenches or tools
421 specified by the manufacturer or supplier shall be used; tools shall not be
422 used that could damage the cylinder, cylinder cap, or valve, or result in the
423 valve being unintentionally opened while the cap is in place.
424
- 425 vii. Screwdrivers shall never be used to pry off a stuck cap.
426
- 427 viii. Pliers shall never be used to open a cylinder valve.
428

429 (c) Maximum Number of Cylinders In a Laboratory or Work Area
430

- 431 i. Only cylinders “in use” may be located in a laboratory or work area. A
432 compressed gas cylinder shall be considered to be “in use” if it is connected
433 through a regulator or to a manifold to deliver gas to an operation. For each
434 such cylinder, a single reserve cylinder may be secured alongside it and
435 considered to be “in use”.¹⁵
436
- 437 ii. Quantities of compressed and liquefied gases in laboratories and work areas
438 shall be in accordance with NFPA 55.¹⁶
439
- 440 (i) The number of lecture-bottle cylinders [approximately 5 cm × 33 cm (2 in.
441 × 13 in.)] in use or reserve shall be limited to 25 per lab or work area.
442

¹⁵ Exceptions to the “alongside” requirement are possible under certain circumstances. See footnote 13.

¹⁶ For assistance in determining quantity limits, contact OSHA at x5375, Option 3

443 (6) Mechanically Ventilated Enclosures and Gas Cabinets

444
445 (a) Lecture bottle-sized cylinders of the following gases located in laboratories shall be
446 kept in continuously mechanically ventilated hoods or other continuously
447 mechanically ventilated enclosures:

448
449 i. All gases that have a NFPA 704 health hazard rating of 3 or 4;

450
451 ii. All gases that have a NFPA 704 health hazard rating of 2 without
452 physiological warning properties such as odor or irritation; and

453
454 iii. Pyrophoric gases.

455
456 (b) Compressed gas cylinders that are larger than lecture bottles and contain the
457 following gases shall be kept in approved continuously mechanically ventilated gas
458 cabinets:

459
460 i. All gases that have a NFPA 704 health hazard rating of 3 or 4;

461
462 ii. All gases that have a NFPA 704 health hazard rating of 2 without
463 physiological warning properties; and

464
465 iii. Pyrophoric gases.

466
467 (c) Gas cabinets shall be constructed in accordance with NFPA 55.

468
469 (d) Gas cabinets shall be used as follows:

470
471 i. Gas cabinets shall contain no more than three containers, cylinders, or tanks;
472 and

473
474 ii. Incompatible gases shall be stored and used in separate gas cabinets.

475
476 (7) Disposition of Empty and No-Longer-Needed Compressed Gas Cylinders

477
478 (a) When a cylinder is emptied to a pressure of 172 kPa (25 psig), the following actions
479 shall be taken:

480
481 i. The regulator shall be removed;

482
483 ii. A valve cap shall be installed;

- 485 iii. The cylinder shall be marked as empty; and
486
487 iv. The cylinder shall be returned to the storage area for pickup.
488
489 (b) If the contents of a cylinder are unknown or appropriate DOT labeling is not present
490 on the cylinder, the cylinder shall not be moved from the laboratory. OSHE shall be
491 contacted to assist with the identification of the cylinder contents and to provide
492 guidance on appropriate disposal procedures.
493
494 (c) Lecture bottles shall not be abandoned in building loading docks or other storage
495 areas.
496
497 (d) Chemical Waste Pick-Up requests shall be submitted to OSHE for pick-up and
498 disposal of empty and no-longer-needed lecture bottles that contained or contain
499 hazardous gases; otherwise, they may be disposed of in the regular trash.
500
501 c. Compressed Gas Vessel and System Design
502
503 (1) System Design
504
505 (a) All systems shall be designed and constructed in accordance with the references listed
506 in Section 4 of this suborder.
507
508 (b) Supply, piping, valves, connections, *etc.*, must be placed in such a way that they can
509 be inspected and will not release into an occupied area without sufficient ventilation
510 to prevent an oxygen-deficient atmosphere.
511
512 (c) If reserve cylinders or back-up supplies are connected, the arrangement shall preclude
513 discharge of reserve cylinders during normal operation of primary supply.
514
515 (d) Systems shall be designed to be free of cross-connections that could allow gas to pass
516 from a section of the system where the gas is intended to be present to a section of the
517 system where the gas is not intended to be present.
518
519 (e) Tubing
520
521 i. Sharp tube bends shall be avoided. Tubing shall not be bent more sharply
522 than recommended by the manufacturer.
523
524 ii. Flexible or plastic tubing shall only be used within "line of sight."
525

iii. Flexible tubing lengths shall be kept as short as possible, shall be protected from mechanical damage, and shall be anchored at the ends to prevent whipping in case of tubing or tube-fitting failure.

iv. Flexible tubing connections shall be secured with clamps approved for the maximum allowable pressure subjected to the connection. Flexible tubing connections shall not be secured with wire.

(f) Valves

i. The number and placement of valves shall be sufficient to facilitate maintenance, and to isolate systems for renovation and in case of emergency.

ii. Continuous access to valves located above ceilings, in utility rooms, or behind equipment shall be maintained.

iii. Valves shall be provided on each line running from a supply line to equipment so the equipment can be isolated for maintenance, repair, or replacement.

iv. Where fuel gas is permitted, a shut-off valve shall be provided immediately adjacent to the safety cabinet or hood or other location where the gas is used.

v. On liquefied-gas systems, all terminal-block (liquid-withdrawal) valves shall:

(i) Be rated above the vapor pressure of the liquid gas at 38°C (100°F); or

(ii) Have properly set relief valves permanently installed on the outlet side of each terminal-block valve.

(g) Gauges

i. Gauges subject to pressure surges or cyclic pulses shall be protected by installing a needle valve or orifice for damping.

ii. When large pressure gauges (over 100 mm in face diameter) are used on gas systems with operating pressures over 1.4 MPa (200 psig) or on liquid systems over 140 MPa (20,000 psig), they shall have a special safety-type design including:

(i) Shatterproof faces;

(ii) Solid fronts; and

(iii) Blowout or generously vented cases.

If a large pressure gauge is used that does not have a special safety-type design, operators must be protected by a Lexan safety shield that is securely mounted over the existing gauge face, or the equivalent.

(h) Flammable Gas-Specific Requirements

- i. Systems using flammable gases shall be designed to prevent a release in concentrations that are within flammable limits.
- ii. Every flammable-gas drop or regulator-tube connection shall be equipped with a flash arrestor, or a check valve, pressure gauge, and shutoff valve. If the flammable gas is to be (or could be) cross-connected with oxygen or compressed air, a flash arrestor shall be installed in the flammable-gas line and a check valve in the oxygen or compressed-air line.

(2) Pipes, Tubing, and Component Materials

- (a) Gas pipes, valves, fittings, regulators, and related components must be constructed of materials compatible with the gases to be contained and must be rated for the service. Stainless steel components are preferred in most systems. Where nonmetallic tubing is approved, additional controls may be required.

(b) Pipes and Tubing

- i. Nonmetallic tubing shall not be used on flammable, toxic, and/or radioactive gas systems.
- ii. Flexible tubing shall not be used for highly toxic gases.

(c) Fittings

- i. Brass fittings shall be used with copper or brass tubing.
- ii. Stainless-steel fittings shall be used with steel or stainless-steel tubing.

(3) Labeling of Gas Lines Emanating from Enclosures

- (a) Each compressed gas line outside of the source gas cabinet or ventilated enclosure must be labeled:

- 610 i. At least every 6 m (20 ft) unless the gas line is shorter than 6 m (20 ft) and the
611 gas line and gas source are in sight;
612
613 ii. At critical shutoff valves;
614
615 iii. At wall, floor, or ceiling penetrations; and
616
617 iv. As otherwise necessary to provide clear identification.
618
- 619 (b) Labels must be durable and display the gas name and direction of gas flow.
620
- 621 (c) Piping that may contain more than one type of gas at various times shall be marked to
622 provide clear identification of that fact.
623
- 624 (4) System Testing
625
- 626 (a) Prior to operation, all newly constructed, newly installed, and remodeled compressed
627 gas systems shall be tested per all applicable codes and standards as well
628 as manufacturer specifications.
629
- 630 (b) Prior to operation, all lines and equipment shall be leak tested with an inert gas.
631
- 632 (5) Inspection and Repair
633
- 634 (a) Flexible tubing shall be inspected for aging, deterioration, and damage with a
635 frequency in accordance with the manufacturer's recommendations.
636
- 637 (b) Any tubing showing leaks, burns, wear, or other defects shall be repaired or replaced
638 immediately. The vessel or system shall not be used until the defective part is
639 repaired or replaced.
640
- 641 (6) Deviations from the Requirements of Sections 6c(1)-(5)
642
- 643 (a) When requirements for specialized compressed gas vessels or systems make it
644 impossible to comply with any of the provisions of Sections 6c(1)-(5), measures must
645 be implemented to provide a level of protection equivalent that provided by these
646 provisions.
647
- 648 (b) Any deviations from these provisions shall be identified as part of the applicable
649 hazard review, and the alternative measures implemented documented therein.
650
- 651 (c) Alternative measures may include the following:

- 652 i. Ventilated enclosures;
653
654 ii. Gas detectors;
655
656 iii. Emergency off buttons;
657
658 iv. Emergency power;
659
660 v. Pneumatic shut-off valves;
661
662 vi. Smoke detectors;
663
664 vii. Fire sprinklers;
665
666 viii. Exhaust scrubbers;
667
668 ix. Flow restrictors; and
669
670 x. Ventilation alarms.
671
- 672 d. Hazardous Material Release
673
- 674 (1) In the case of an accidental or uncontrolled release of a hazardous compressed gas, the
675 individual that discovers the release shall warn others in the immediate area, move to a
676 safe location, and report the leak.
677
- 678 (a) In Boulder, the incident shall be reported by dialing 911 for Boulder Fire-Rescue and
679 x7777 for NIST Police.
680
- 681 (b) In Gaithersburg, the incident shall be reported by dialing x2222 for NIST Emergency
682 Services.
683
- 684 (c) Ignition sources in the vicinity of leaking flammable gas should be turned off if it is
685 obvious that this can be done safely.
686
- 687 e. Training
688
- 689 (1) Training provided by OSHE on the Compressed Gas Safety Program and activity-specific
690 training required by applicable hazard reviews shall be assigned and documented, and its
691 completion by affected employees and associates recorded, in accordance with the
692 requirements, roles, and responsibilities of NIST S 7101.23: Safety Education and
693 Training. In particular:

(a) Employees and associates who are to engage in activities involving compressed gases shall complete:

- i. The training provided by OSHE on the Compressed Gas Safety Program; and
- ii. The activity-specific training, provided by their Organizational Units, required by applicable hazard reviews.

(b) The official first-level supervisors of employees and associates who are to engage in activities involving compressed gases shall complete the training provided by OSHE on the Compressed Gas Safety Program.

7. DEFINITIONS

- a. Asphyxiant – A material capable of reducing oxygen in a person's body to dangerous levels, most commonly caused by displacing breathable air in an enclosed environment.
- b. Ceiling Limit – An occupational exposure limit that should not be exceeded during any part of the working exposure. If instantaneous exposure levels cannot be determined, an average exposure over a 15-minute time period is generally used.
- c. Compressed Gas – A material, or mixture of materials, that (1) is a gas at 20°C (68°F) or less at an absolute pressure of 101.325 kPa (14.696 psia) and (2) that has a boiling point of 20°C (68°F) or less at an absolute pressure of 101.325 kPa (14.7 psia) and that is liquefied, non-liquefied, or in solution, except those gases that have no other health or physical hazard properties are not considered to be compressed gases until the pressure in the packaging exceeds an absolute pressure of 280 kPa (40.6 psia) at 20°C (68°F).
- d. Compressed Gas Cylinder (Cylinder) – A pressure vessel designed for pressures higher than 276 kPa (40 psia) and having a circular cross-section. It does not include a portable tank, multiunit tank car tank, cargo tank, or tank car.
- e. Corrosive Gas – A gas that causes visible destruction of, or irreversible alterations in, materials or living tissue by chemical action at the site of contact.
- f. Design Pressure – The maximum pressure at which a vessel or the weakest member of a pressure system has been designed to safely function at the normal operating temperature. Also the maximum setting of a pressure-relief device on a vessel or pressure system.
- g. Flammable Gas – Any substance that exists in the gaseous state at normal atmospheric temperature and pressure, and is capable of being ignited and burned when mixed with the proper proportions of air, oxygen, or other oxidizers.

- h. Highly Toxic Gas – A gas that can kill 50 percent of the test subjects (LC₅₀) with a concentration of less than or equal to 200 parts per million (ppm), a gas that has an ACGIH TLV or OSHA PEL of one ppm or less, or a gas designated as a “Poison A” by the DOT and defined as a poisonous gas of such nature that a very small amount of the gas mixed with air is dangerous to life. Lists of LC₅₀ values for toxic gases and vapors are available in ISO 10298. (An NFPA 704 Health Hazard rating of 4 is given to gases having an LC₅₀ in air of less than or equal to 1000 ppm.)
- i. Hydrostatic Test – A test of the strength and leak-resistance of a compressed gas cylinder by internal pressurization with a test liquid.
- j. Immediately Dangerous to Life or Health (IDLH) – Defined by NIOSH as exposure to airborne contaminants that is "likely to cause death or immediate or delayed permanent adverse health effects or prevent escape from such an environment.”
- k. Material Safety Data Sheet (MSDS/SDS) – A document produced by chemical manufacturers or importers in accordance with 29 CFR 1910.1200 to relay chemical, physical, and hazard information about specific substances.
- l. Nesting – A method of securing flat-bottom cylinders upright in a tight mass using a contiguous three-point contact system whereby all cylinders within a group have a minimum of three points of contact with other cylinders, walls, or bracing (see CGA P-1, Appendix A).
- m. Operating Pressure – The maximum pressure at which a vessel or pressure system is intended to be used under normal circumstances. This will generally be 5 percent to 25 percent lower than the design pressure for systems protected by a spring-loaded relief device and approximately 33 percent lower than the design pressure for systems protected by rupture-disk relief devices, depending on the fatigue life of the disc used, the temperature, and load pulsation.
- n. Oxidizing Gas – A gas that can initiate or support combustion, and can accelerate the combustion of other materials.
- o. Oxygen-Deficient Atmosphere – An atmosphere containing less than 19.5 percent oxygen by volume.
- p. Permissible Exposure Limit (PEL) – A legally-enforceable occupational exposure limit established by OSHA that sets the maximum time-weighted average concentration of an air contaminant that workers may be exposed to over an 8-hour workday of a 40-hour workweek.

- q. Pressure Relief Valve – A device designed to open at a predetermined pressure in order to prevent an unsafe rise of internal pressure in a pressure vessel or system.
- r. Pyrophoric Gas – A chemical in a gaseous state that will ignite spontaneously in air at a temperature of 130 degrees F (54.4 degrees C) or below.
- s. Regulator – A device that controls the release of gas from cylinders or other vessels.
- t. Storage Area – A designated area, either indoors or outdoors, where cylinders that are not being used, loaded, or unloaded are stored safely for future use, and to which cylinders that are empty are returned for pickup.
- u. Threshold Limit Value (TLV) – A recommended occupational exposure limit established by ACGIH, which is the time-weighted average of a contaminant to which nearly all workers may be repeatedly exposed day after day without adverse health effects
- v. Toxic Gas – A gas with an LC₅₀ between 200 ppm to 2,000 ppm, or a gas that has an ACGIH TLV or OSHA PEL between 1 ppm to 50 ppm. Lists of LC₅₀ values for toxic gases and vapors are available in ISO 10298. (An NFPA 704 Health Hazard rating of 3 is assigned to gases having LC₅₀ air concentrations between 1,000 ppm to 3,000 ppm.)
- w. Transfiling – Transfer of compressed gas from one container to another.

8. ACRONYMS

- a. ACGIH – American Conference of Governmental Industrial Hygienists
- b. CFR – Code of Federal Regulations
- c. CGA – Compressed Gas Association
- d. CSO – Chief Safety Officer at NIST
- e. DOT – Department of Transportation
- f. IDLH – Immediately Dangerous to Life and Health
- g. ISO – International Organization for Standardization
- h. LC₅₀ – Lethal Concentration 50 Percent
- i. NFPA – National Fire Protection Association

j. NIOSH – National Institute of Occupational Safety and Health

k. OSHA – Occupational Safety and Health Administration

l. OSHE – NIST Office of Safety, Health, and Environment

m. PEL – Permissible Exposure Limit

n. TLV – Threshold Limit Value

9. RESPONSIBILITIES

a. OU Directors are responsible for:

(1) Ensuring that the requirements of Section 6 of this suborder are met in their OUs; and

(2) Determining which OU or division in an OU is responsible for managing gas cylinder storage areas shared by multiple OUs.¹⁷

b. Division Chiefs are responsible for:

(1) Submitting requests for exceptions to the following requirements based on an evaluation of programmatic need:

(a) Section 6b(4)(a)i regarding the storage of compressed gas cylinders in laboratories;

(b) Section 6b(4)(c)i-ii regarding the storage of compressed gas cylinders in loading docks at NIST Gaithersburg, in consultation with the Storeroom; and

(c) Section 6b(5)(c)i regarding reserve cylinders being alongside cylinders in use.

c. OSHE is responsible for:

(1) Approving or disapproving requests for the exceptions listed above.

d. Storeroom Supervisor is responsible for:

(1) Ensuring that compressed cylinders delivered to the Storeroom by outside vendors are inspected in accordance with the requirements of Section 6b(2) on point-of-delivery inspection of compressed gas cylinders;

¹⁷ For example, this responsibility could be assigned to the OU that is the heaviest user of gas cylinders in a particular storage area, or to a division in that OU.

- 859 (2) Delivering full compressed gas cylinders to building loading docks per customer orders;
860
861 (3) Not delivering compressed gas cylinders to building loading docks when storage rack
862 areas are unavailable to secure the cylinders safely;
863
864 (4) Ensuring that cylinders of normally-stocked gases stored in building loading docks for
865 more than 30 days are returned to the storeroom;
866
867 (5) Ensuring that cylinders of non-stocked (special order) gases stored in building loading
868 docks for more than 90 days are returned to the storeroom and then to the supplier; and
869
870 (6) Consulting with the OSHE on the approval or disapproval of requests for exceptions to
871 the requirements of Section 6b(4)(c)i-ii I regarding the storage of compressed gas
872 cylinders in loading docks at NIST Gaithersburg.
873
874

875 **10. AUTHORITIES**

876 There are no authorities specific to this suborder.
877
878

879 **11. DIRECTIVE OWNER**

880 Chief Safety Officer
881
882

883 **12. APPENDICES**

884 a. Appendix A. Revision History
885

886
887

888

SAFETY IN OFFICES AND OFFICE-LIKE SPACES (“OFFICE SAFETY”)

NIST S7101.62

Document Approval Date: 04/07/2016

Effective Date:^{1,2} 04/01/2016

1. PURPOSE

The purpose of this program is to establish the safety requirements necessary to protect the safety and health of employees and associates in offices³ and office-like spaces⁴.

2. BACKGROUND

- a. [NIST P 7100.00: Occupational Safety and Health Policy](#) articulates NIST’s commitment to making occupational safety and health an integral core value and vital part of the NIST culture by, in part, complying with applicable laws, regulations, and other promulgated safety and health requirements.
- b. NIST must meet the requirements of the [Occupational Safety and Health Act](#) (OSH Act), which requires employers to provide their employees with working conditions that are free of recognized hazards that are causing or are likely to cause death or serious physical harm. Implementation of this suborder through the requirements in Section 6 and roles and responsibilities in Section 9 of this document fulfills those requirements for offices and office-like spaces.

¹ For revision history, see Appendix A.

² All requirements in this suborder except for the portable electric space heater requirements in Section 6d(4) were effective on 04/01/16. The portable electric space heater requirements in Section 6d(4) will be effective on 10/01/2016 in accordance with [NIST N 7101.62, Portable Electric Space Heaters](#).

³ An office is defined as a workspace where administrative duties such as reading, writing, telephone use, and computer use are performed. Types of offices include private office, shared office, cubicle, and open office.

⁴ An office-like space is defined as a space, such as a conference room, copier room, break room, or ordinary computer room that has the same types of hazards as a typical office or office environment.

- c. Indoor air quality in offices and office-like spaces is addressed in the Industrial Hygiene Suborder.

3. APPLICABILITY

- a. The provisions of this suborder apply to:

- (1) All offices and office-like spaces at NIST and non-NIST sites;⁵ and
- (2) All activities conducted by NIST employees and associates in offices and office-like spaces that are not subject to the requirements of [NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews](#) (“Hazard Review”), that is:
 - (a) Common everyday tasks performed routinely by members of the general public at work and home and that do not involve extraordinary hazards; and
 - (b) Activities that present inherently low safety risks.

- b. The provisions of this suborder do not apply to residential work locations (e.g., telework).

4. REFERENCES

- a. [Occupational Safety and Health Act, Section 5\(a\)\(1\) \(“General Duty Clause”\)](#).
- b. [29 CFR 1910](#), Subpart L, Fire Protection and Subpart S, Electrical.
- c. [29 CFR 1910, Subpart D, Walking-Working Surfaces](#), especially Sections 1910.22, General Requirements.
- d. [29 CFR 1910.141, Sanitation](#).
- e. [NIST O 7101.00: Occupational Safety and Health Management System](#).
- f. [NIST P 7100.00: Occupational Safety and Health Policy](#).

⁵A non-NIST site is an off-site non-residential workplace owned and operated by an entity other than NIST at which NIST employees and associates carry out their assigned duties. Examples include joint institutes such as JILA in Boulder, CO, the Hollings Marine Laboratory in Charleston, SC, and Joint Quantum Institute in College Park, MD.

66 **5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS**

- 67 a. [NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews \(Hazard](#)
68 [Review”\)](#)
69
70 b. [NIST S 7101.22: Hazard Signage](#)
71
72 c. [NIST S 7101.23: Safety Education and Training](#)
73
74 d. [NIST S 7101.26: Workplace Inspection](#)
75
76 e. [NIST N 7101.62, Portable Electric Space Heaters](#)
77
78 f. [NIST S 7101.71: Industrial Hygiene](#)
79
80 g. [NIST S7101.75: Walking/Working Surfaces](#)
81
82

83 **6. REQUIREMENTS**

84 a. Housekeeping

- 85
86 (1) Offices and office-like spaces should be kept clean and dry.
87
88 (2) Items shall not be located or stored where they would present slipping or tripping hazards
89 or hinder an evacuation.
90
91 (3) Cords that hang/dangle underneath desk and/or tables should be secured with cable ties to
92 prevent tripping hazard.
93
94 (4) Drawers on desks and file cabinets shall be closed when not in use to prevent tripping and
95 struck-against incidents.
96
97 (5) Stacked items should be kept below eye level to avoid struck-by incidents;
98
99 (6) Heavy or bulky items should be stored at lower levels or in a manner that minimizes their
100 potential to fall or cause shelving, bookcases, file cabinets, or other types of furniture to
101 topple. “Heavy or bulky” pertains to the potential for physical injury if the items were to
102 fall or the furniture to topple. Loading on furniture shall not exceed manufacturers’
103 stated limits.
104
105

(7) Items should not be located or stored where they block ventilation.

b. Walking/Working Surfaces

(1) Loose, damaged, slippery, or uneven flooring should be reported as soon as possible for repair or replacement.⁶

(2) Cord guards covering cords positioned across walkways shall be secured in such a manner as to avoid tripping hazards [see also Section 6d(1)(f)]. Cord guards shall not be covered with mats or rugs.

(3) Floor mats shall be non-sliding and in good condition with edges lying flat.

c. Step Stools and Small Step Ladders

(1) Step stools or small step ladders should be used to reach elevated objects

NOTE: Office furniture, such as chairs and desks, should not be used.

(2) Step stools and small step ladders shall have anti-slip feet.

(3) Step stools and small step ladders should have hand rails when over 2-steps.

(4) Step stools and small step ladders shall be maintained in good condition, inspected before each use, and used in accordance with manufacturers' instructions.

d. Electrical Safety

(1) General

(a) When in use, electrical cord plugs of any kind shall be fully inserted into receptacles such that the plugs' metal prongs are not showing.

(b) Three-prong to 2-prong plug adapters shall not be used.

(c) Tension on electrical cords plugged into receptacles shall be avoided.

⁶ In Gaithersburg, Boulder, and Fort Collins, a [Maintenance Request \(M-Slip\)](#) shall be submitted to OFPM requesting repair or replacement. At sites owned and operated by entities other than NIST, requests shall be submitted to the responsible entity.

(d) Cords, cables, and/or wires shall not be pinched.

(e) Flexible cords and cables shall be not attached to building surfaces as permanent installations.

(f) Cord guards shall be used to protect flexible cords positioned across walkways from wear and tear caused by foot and other traffic [see also Section 6b(2)].

(g) Cords with damaged plugs (*e.g.*, broken, cracked, or missing prongs or ground pins) or exposed wire shall be removed from service immediately and discarded, or if they are part of a piece of equipment, that equipment shall not be used until the cord has been replaced.

(2) Permanently-Installed Electrical Outlets

(a) The load on permanently-installed electrical outlets shall not exceed 16 amperes (1920 Watts) for 20-amp circuits or 12 amperes (1440Watts) for 15-amp circuits.^{7, 8}

(b) Permanently installed electrical outlets with broken, missing, and/or cracked cover plates shall be:

i. Covered and not used; and

ii. Reported as soon as possible for repair or replacement.⁴

(c) If permanent electrical outlets or other electrical receptacles are within six (6) feet (183 centimeter) of a water source in wet locations, such as a kitchen or break room, ground-fault-circuit-interrupter (GFCI) protections shall be installed.⁶ This protection may be provided at the receptacle itself, in an upstream device such as another receptacle, or as a GFCI circuit breaker in the electrical distribution panel.

⁷ Most circuits in offices and office-like spaces at NIST are 20-ampere circuits, but some are 15-ampere circuits. If you wish to attach more than a 12-ampere (1440 W) load and you are not sure if the circuit is 20-ampere circuit, contact OSHE on x5375, Option 3.

⁸ If additional outlets or GFCI protection are required in Gaithersburg, Boulder, or Fort Collins, OU-funded work orders ([Form NIST-260](#)) shall be submitted to the Office of Facilities and Property Management (OFPM) to have additional outlets or GFCI protection installed. If additional outlets or GFCI protection are required at sites owned and operated by entities other than NIST, requests shall be submitted to those entities to have additional outlets or GFCI protection installed.

176 (3) Supplemental Power Devices
177

- 178 (a) Supplemental power devices, such as power strips, surge suppressors, uninterruptible
179 power supplies (UPS), and extension cords, shall bear the mark of a Nationally
180 Recognized Testing Laboratory, such as Underwriters Laboratories (UL) or Factory
181 Mutual.
182
- 183 (b) Only supplemental power devices that are grounded shall be used. Grounded cords
184 have three prongs on their plugs, rather than two.
185
- 186 (c) Supplemental power devices shall be connected directly to permanently-installed
187 electrical outlets (no “daisy chaining” or “piggybacking” to other supplemental power
188 devices).⁶
189
- 190 (d) Supplemental power devices shall be used and stored according to the manufacturers’
191 safety instructions.
192
- 193 (e) Supplemental power devices shall be mounted according to the manufacturers’
194 instructions.
195
- 196 (f) Supplemental power devices shall not be secured to building structures (walls,
197 columns, ceilings, and floors) with tape, zip-ties, nails, or other fastening devices that
198 require tools such as screw driver, knife, scissors, etc. for removal.
199
- 200 (g) Extension cords shall not be used as substitutes for permanent wiring and shall be
201 unplugged and properly stored after use.⁶
202
- 203 (h) Supplemental-power-device cords shall not be routed through walls, floors, windows,
204 doorways, or ceilings where they cannot be inspected and could be unknowingly
205 damaged.
206
- 207 (i) Damaged supplemental power devices, such as those with exposed electrical
208 conductors or wires, shall be repaired by the manufacturer (or similar qualified
209 service provider) or discarded immediately.
210
- 211 (j) Power strips, surge suppressors, or UPSs shall not be opened unless the operator’s
212 manual provided by the manufacturer allows and includes instructions for doing it.
213

(k) The working space around serviceable electrical panels⁹ shall be kept clear at all times of moveable objects such as furniture, equipment, materials, etc.¹⁰

i. The working space shall permit at least a 90-degree opening of hinged panels.

(l) If the working space around a serviceable electrical panel contains permanently installed structural members such as walls, columns, work surfaces, etc.), the condition shall be reported to OSHE on x5375, Option 3.¹¹

(4) Appliances

(a) Manufacturers' safety instructions shall be followed for appliances used in offices and office-like spaces

(b) Electrical appliances that have current loads greater than 12 amperes (power loads greater than 1440 Watts), such as space heaters, refrigerators, and microwave ovens, shall be plugged directly into permanently installed electrical outlets or any power strip that is listed for commercial or industrial applications, has a master circuit breaker, a master power switch, and a metal case.¹² Extension cords, regardless of length, may not be used with electrical appliances with high power loads.

(c) Electrical appliances with heating elements, such as portable electric space heaters, coffee pots, toasters, and toaster ovens shall meet the following technical and usage requirements:

i. They shall bear the mark of a [Nationally Recognized Testing Laboratory](#) (NRTL), such as Underwriters Laboratories (UL) or Factory Mutual;^{13, 12}

⁹See definition of "Working Space". It is presumed that electrical panels in NIST offices and office-like spaces are supplied by 150 volts or less. If panels are supplied by greater than 150 volts, the depth of the access in front of the panel must be at least 42 inches (1.07 m) in the direction of the panel.

¹⁰ In the future, the working space shall also be kept clear of permanently installed structural members such as walls, columns, work surfaces, etc. This is purview of the responsible facilities organization, and, as such, is outside the scope of this suborder.

¹¹ OSHE and the Office of Facilities and Property Management (OFPM) will (a) evaluate the condition to determine what actions need to be taken to protect workers and ensure regulatory compliance, and (b) ensure those actions are taken or planned.

¹² Contact OSHE on x5375, Option 3 for a list of acceptable power strips.

¹³ Appliances brought to NIST from outside the U.S. warrant attention. For assistance, contact OSHE on ext. 5375, Option 3.

¹² A label representing that a product "conforms" to a standard is not a sufficient replacement for the mark of a NRTL.

- 242 ii. They shall be plugged directly into permanently installed electrical outlets or any
243 power strip that is listed for commercial or industrial applications, has a master
244 circuit breaker, a master on/off switch, and a metal case.¹⁰ Extension cords,
245 regardless of length, may not be used with electrical appliances with heating
246 elements.
- 247
- 248 iii. Manufacturers' clearance requirements around coffee pots, toasters, and toaster
249 ovens shall be followed.
- 250
- 251 iv. When in use, toaster ovens shall not be left unattended.
- 252
- 253 v. Combustible materials (furniture, paper, and household consumer products) shall
254 be kept at least 3 feet (0.9 m) from the front of portable electric space heaters and
255 away from their back and sides.
- 256
- 257 vi. Portable electric space heaters shall be equipped with a safety tip-over switch
258 that will shut off the heater when tipped over.
- 259
- 260 vii. Portable electric space heaters shall have a thermal cutoff feature that will shut
261 off the heater upon detection of abnormal temperature conditions.
- 262
- 263 viii. Portable electric space heaters shall have an adjustable temperature controller
264 incorporating a thermostat to cycle the heater based on surrounding temperature.
- 265
- 266 e. Fire Safety
- 267
- 268 (1) No open flames such as lit candles and portable propane burners shall be allowed in
269 offices or office-like spaces. Burning incense is also not allowed.
- 270
- 271 (2) Fire-Related Storage
- 272
- 273 (a) Flammable or combustible chemicals, other than household consumer products and
274 personal items such as disinfectant wipes, disinfectant gel, rubbing alcohol, hairspray,
275 nail polish, nail polish remover, and personal medication (inhalers), shall not be
276 stored in offices or office-like spaces.
- 277
- 278 (b) Stored materials in non-sprinklered areas shall be at least 24 inches (0.61 m) from the
279 ceiling.
- 280

NOTE: This requirement does not apply to materials stored on shelves against walls unless determined by OSHE to be unsafe.

- (c) Stored materials in sprinklered areas shall be at least 18 inches (0.46 m) below the height of the sprinkler heads.

NOTE: Exemptions from this requirement are possible under certain circumstances. OSHE must be contacted for the approval of any storage or storage design that deviates from the requirement.

- (3) Exit paths shall be at least 28 inches (0.71 m) wide for small office spaces (no more than six occupants).¹⁴

- (4) Exits paths shall be clear of obstructions.

f. Office Equipment/Furniture

- (1) Copiers, printers, paper shredders, and other office equipment shall be placed and used according to manufacturers' instructions. In common-use spaces, manufacturers' instructions shall be easily accessible to all users.

- (2) Paper cutters shall be equipped with finger-guard rails and located on flat stable surfaces. Blades shall be latched when not in use.

NOTE: Rotary trimmers are excluded.

- (3) Box cutters with recessed blades should be used.

- (4) Equipment and furniture with sharp edges should be protected with edge guards where applicable.

- (5) Furniture that could fall or topple should be secured to walls.

g. Office Chemicals

- (1) Hazardous chemicals other than household consumer products and personal items [see Section 6e(2)(a)] shall not be stored in offices or office-like spaces.

¹⁴ Contact OSHE on x5375, Option 3 for specific exit widths for other office spaces.

(2) Consumer products such as “Windex”, correction fluid, adhesives, board cleaners, and copier/printer toners and inks are permitted in office and office-like spaces provided that the products are used in these areas in the same manner that a consumer would use them, *i.e.*, where the duration and frequency of use is not greater than what the typical consumer would experience.

h. Ergonomics

(1) Employees shall have the right to receive OSHE-provided ergonomic assessments to address office ergonomic risk factors, *i.e.*, elements of their jobs, or the methods by which their jobs are performed, that could contribute to the development of musculoskeletal injuries.

(2) Heavy items that must be lifted should be stored at waist height, when possible.

i. Lighting

(1) Non-functional lighting that presents a safety hazard should be reported as soon as possible for repair or replacement.⁴

(2) Work stations and computer monitors should be positioned to reduce glare.

(3) Where appropriate, task lighting should be used.

7. DEFINITIONS

a. Non-NIST Site – An off-site non-residential workplace owned and operated by an entity other than NIST at which NIST employees and associates carry out their assigned duties. Examples include joint institutes such as JILA in Boulder, CO, the Hollings Marine Laboratory in Charleston, SC, and Joint Quantum Institute in College Park, MD.

b. Office – A workspace where administrative duties such as reading, writing, telephone use, and computer use are performed. Types of office include private office, shared office, cubicle, and open office.

c. Office-Like Space – A space, such as a conference room, copier room, break room, or ordinary computer room that has the same types of hazards as a typical office or office environment.

- d. Supplemental Power Devices – Power strips, surge suppressors, uninterruptible power supplies (UPS), and extension cords. Chargers for portable computers and mobile devices are not supplemental power devices as defined herein.
- e. Working Space (around serviceable electrical panels) – A space around a serviceable electrical panel with the following dimensions:
- (1) A depth in the direction of access to the panel of at least 36 inches (0.91 m) from the front of the panel;
 - (2) A width in front of the panel of 30 inches (0.76 m) or the width of the panel, whichever is greater; and
 - (3) A height from the floor or platform to 6 feet 6 inches (1.98 m) or the top of the panel, whichever is greater.

8. ACRONYMS

- a. CFR – Code of Federal Regulations
- b. NRTL – Nationally Recognized Testing Laboratory
- c. OFPM – Office of Facilities and Property Management
- d. OSHA – Occupational Safety and Health Administration
- e. OSHE – Office of Safety, Health, and Environment
- f. OU – Organizational Unit
- g. UPS – Uninterruptible power supplies

9. RESPONSIBILITIES

Roles and responsibilities specific to this suborder are as follows:

- a. OU Directors are responsible for ensuring that the requirements of this suborder are met in their offices and office-like spaces.

398 **10. AUTHORITIES**

399 There are no authorities specific to this suborder alone.

400

401

402 **11. DIRECTIVE OWNER**

403 Chief Safety Officer

404

405

406 **12. APPENDICES**

407 a. Revision History

408

409

410
411

Appendix A. Revision History

Revision No.	Approval Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	04/15/15	04/22/15	04/01/16	None – Initial document
1	04/07/16	NA	04/07/16	<ul style="list-style-type: none"> Replaced requirement in Section 6d(4) that appliances be “kept a minimum of 3 feet (0.91m) away from combustible and flammable materials” with (a) “Manufacturers’ clearance requirements around coffee pots, toasters, and toaster ovens shall be followed”, “When in use, toaster ovens shall not be left unattended”, and “Combustible materials (furniture, paper, and household consumer products) shall be kept at least 3 feet (0.9 m) from the fronts of portable electric space heaters and away from their back and sides.” Added additional safety requirements for portable electric space heaters to Section 6d(4) in accordance with NIST N 7101-62, Portable Electric Space Heaters.

412

Electrical Safety

NIST S 7101.64

Effective Date: 10/23/2015

Document Approval Date: 10/23/2015

1. PURPOSE

This Notice establishes the requirements, roles, responsibilities, and authorities for performing energized electrical work, including electrical lockout/tagout (electrical LOTO). It will remain in place from its issuance date until the effective date of NIST Suborder (S) 7101.64: Electrical Safety.

NOTE: NIST expects NIST S 7101.64: Electrical Safety to be effective on April 1, 2017, with deployment commencing in the 3rd quarter of FY 2016. NIST S 7101.64 will incorporate the requirements of this notice.

2. BACKGROUND

- a. Energized electrical work, including electrical LOTO, can present significant electrical-shock and arc-flash hazards absent implementation of the safety requirements herein.
- b. The contents of this Notice are based on the current editions of Occupational Safety and Health Administration (OSHA) standards in 29 CFR 1910, Subpart S, Electrical, and National Fire Protection Association (NFPA) codes/standards NFPA 70, 70B, and 70E.

3. APPLICABILITY

- a. The requirements of this Notice apply to the following, regardless of the physical location in which the work is being performed:
 - (1) NIST employees and associates who could be exposed to electrical hazards, e.g., shock, arc flash, while performing energized electrical work, including electrical LOTO, in the performance of their duties; and

- (2) NIST employees who are responsible for outside service providers performing energized electrical work, including electrical LOTO, and as such, are responsible for ensuring that other NIST employees and associates are not exposed to the hazards of that work.

4. REFERENCES

- a. OSHA 29 CFR 1910 Subpart S, Electrical
- b. NFPA 70, National Electric Code, current edition
- c. NFPA 70B, Recommended Practice for Electrical Equipment Maintenance, current edition
- d. NFPA 70E, Electrical Safety in the Workplace, current edition

5. APPLICABLE NIST OCCUPATIONAL SAFETY AND HEALTH SUBORDERS

- a. [NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews](#);
- b. [NIST S 7101.21: Personal Protective Equipment](#); and
- c. [NIST S 7101.56: Control of Hazardous Energy \(Lockout/Tagout\)](#).

6. REQUIREMENTS

[Section 6a](#) delineates conditions under which work on electrical equipment and circuits may be conducted in an energized state. [Sections 6b](#) and [6c](#) delineate the requirements for de-energizing and re-energizing, respectively, equipment and circuits. [Sections 6d](#) and [6e](#) delineate the requirements for performing energized electrical work without and with, respectively, an Energized Electrical Work Permit ([EEWP](#); see Section 7, Definitions).

- a. Conditions under which Work on Electrical Equipment and Circuits May Be Conducted in an Energized State
 - (1) Work on electrical, electronic, and electro-mechanical equipment and circuits shall be performed in a de-energized state unless at least one of the following conditions is met:
 - (a) Energized electrical conductors and circuit parts to which employees and associates could be exposed operate at less than 50 volts and no other electrical hazards, e.g., potential for electrical burns or explosion, exist;

- (b) It can be demonstrated to the responsible OU management that de-energizing would introduce additional hazards, would introduce increased risk, or could cause significant property damage or loss of critical data;¹
- (c) It can be demonstrated to the responsible OU management that performing the work in a de-energized state is infeasible (not just inconvenient) due to equipment design or operational limitations;² or
- (d) Normal operation of equipment or circuits for their intended purpose(s) provided the equipment or circuits and any upstream protective devices are known to be properly installed and maintained.

b. De-Energizing Electrical Equipment or Circuits to Perform Work

This section applies to de-energizing electrical equipment or circuits and verifying zero energy in the process of performing electrical LOTO. It does not apply to:

- Work on electrical conductors and circuit parts that operate at less than 50 volts provided no other electrical hazards exist; or
- When equipment is to be taken out of service and workers will not be exposed to electrical hazards.

(1) Electrical LOTO shall be conducted in accordance with the requirements in Section 6 of [NIST S 7101.56, *Control of Hazardous Energy \(Lockout/Tagout\)*](#) and the requirements delineated in the remainder of this subsection.

(2) Instructions for de-energizing equipment or circuits shall include procedures for:

- (a) Disconnecting equipment and circuits to be worked on from all electric energy sources;

¹ For example, as in the case of interruption of life-support systems or mission-critical equipment or research, deactivation of emergency alarm systems, and shutdown of hazardous location ventilation equipment.

² For example, as in the case of diagnostics that can only be performed with the circuit energized, and work on circuits that form an integral part of a continuous process that would otherwise need to be shut down completely to allow work on one circuit or piece of equipment.

- i. Control circuit devices, such as push buttons, selector switches, and interlocks, shall not be used as the sole means for de-energizing equipment or circuits;³
 - (b) Releasing from components⁴ stored electric energy that might endanger personnel;
 - i. Capacitors shall be discharged; and
 - ii. High-capacitance elements shall be short-circuited and grounded;
 - (c) Blocking stored non-electrical energy in devices that could re-energize electric circuit parts; and
 - (d) Performing electrical LOTO, including steps for inhibiting automatic and remotely activated functionality.
- (3) Locks and tags used in conducting electrical group LOTO shall:
- (a) Have a distinguishing identifier to identify it as an electrical group LOTO lock;
 - (b) Locks shall not be keyed alike except to a single master for each work group; and
 - (c) Each lock shall be individually numbered.
- (4) A lock and a tag shall be placed on each disconnecting means used to de-energize equipment and circuits on which work is to be performed. The lock shall be attached so as to prevent persons from operating the disconnecting means unless they resort to undue force or the use of tools.
- (a) Equipment with a source voltage of 240 volts or less fed by a single cord and plug shall not be required to have a lock and tag on the plug provided that all hazardous energy to which the worker could be exposed is controlled by unplugging the equipment and the plug is under the exclusive control of the worker. Such equipment shall have a lock and tag applied to the plug when workers are not present and there are exposed electrical circuits, components, or parts.
- (5) A tag may be placed without a lock only if a lock cannot be applied or ALL of the following conditions are met:

³ Exceptions may be possible for laboratory test equipment with built-in mechanisms designed to de-energize the output and control the electrical hazards associated with the normal use of the equipment. Contact the OSHE Electrical Safety Engineer for further information.

⁴ If the components, such as the capacitors, or associated equipment are handled in meeting this requirement, they shall be treated as energized.

- (a) Only one piece of equipment or one circuit is de-energized;
 - (b) The tag is supplemented by at least one additional safety measure that provides a level of safety equivalent to that obtained by the use of a lock, as determined by the OSHE Electrical Safety Engineer ([ESE](#));⁵
 - (c) The lockout period does not extend beyond the work shift; and
 - (d) Employees and associates exposed to the hazards associated with re-energizing the equipment or circuit are trained in this procedure.
- (6) An interlock for electric equipment may not be used as a substitute for written electrical LOTO procedures except in a [laboratory](#) (see Section 7, Definitions) or in an installation designated for research-and-development ([R&D](#)) (see Section 7, Definitions) when all of the following conditions are met:
- (a) The electrical LOTO is part of a laboratory or R&D activity;
 - (b) The interlock is supplemented with a written procedure resulting from an approved OU hazard review; and
 - (c) Proper PPE is worn in accordance with the procedure resulting from an approved OU hazard review.
- (7) The following requirements for verifying the de-energized condition shall be met before any equipment can be considered and worked on as de-energized:
- (a) A [qualified person](#) (see Section 7, Definitions) shall operate the equipment operating controls or otherwise verify that the equipment cannot be restarted.
 - (b) A qualified person shall use test equipment to verify that electrical parts of equipment and circuit elements to which employees or associates will be exposed are de-energized.
 - (c) A qualified person shall use test equipment to determine if any energized condition exists as a result of inadvertently induced voltage or unrelated voltage back-feed even though specific parts of the circuit have been de-energized and presumed to be safe.

⁵ Examples of additional safety measures include the removal of an isolating circuit element, blocking of a controlling switch, or opening of an extra disconnecting device.

- (d) For voltages below 600 volts or when it has been determined that there are no voltages over 600 volts, a voltmeter or multimeter on the appropriate range/scale shall be used by a qualified person to verify zero volts phase-to-phase and phase-to-ground for all source phases. Testing shall be as follows:
 - i. The meter shall be tested on a known source of the same voltage as that being verified for zero electrical energy;
 - ii. The meter shall be used to test the equipment for zero electrical energy; and
 - iii. The meter shall be tested again on a known source of the same voltage as that being verified for zero electrical energy.
- (e) Until it is determined that the voltage level is 600 volts or less, it shall be assumed that the voltage is above 600 volts and special voltage measuring devices rated for the anticipated voltages shall be used when taking voltage measurement.
- (f) Proximity testers or “tic tracers” shall not be used to verify zero volts in the performance of electrical LOTO.
- c. Re-Energizing Electrical Equipment or Circuits
 - (1) The following requirements for re-energizing equipment or circuits shall be met, in the order given, before equipment or circuits are re-energized:
 - (a) A qualified person shall conduct tests and visual inspections, as necessary, to verify that all tools, electrical jumpers, shorts, grounds, and other such devices have been removed.
- d. Energized Electrical Work Not Requiring an [EEWP](#)
 - (1) Energized electrical work may be performed *without* an [EEWP](#) (see Section 7, Definitions) provided the qualified person conducting the work:
 - (a) Has been trained on the appropriate safe work practices associated with the task(s);
 - (b) Uses the required personal protective equipment (PPE) in accordance with Appendices B through G to perform the task(s); and
 - (c) Performs one of these types of tasks:

- i. Work on energized electrical conductors and circuit parts operate at less than 50 volts and no other electrical hazards exist;
 - ii. Diagnostics, i.e., taking readings or measurements of electrical equipment with approved test equipment that do not require making any physical changes to the equipment;
 - iii. Thermography and visual inspections if the restricted approach boundary is not crossed;
 - iv. Tasks involving access to and egress from an area with energized electrical equipment or circuits if no energized electrical work is performed and the restricted approach boundary is not crossed; or
 - v. General housekeeping and miscellaneous non-electrical tasks if the restricted approach boundary is not crossed and all automatic/remotely activated controls are inhibited.
- (2) Energized electrical work that can be performed without an [EEWP](#) must still be authorized in accordance with the requirements of [NIST S 7101.20: Work and Worker Authorization Based on Hazard Reviews](#).
- e. Energized Electrical Work Requiring an [EEWP](#) (a.k.a. Permit-Required Energized Electrical Work)
- (1) The following types of energized electric work may be conducted only in accordance with the requirements of an authorized [EEWP](#), as described in Section 6f:
- (a) Work, other than that described in Section 6d, requiring the qualified person to work within the restricted approach boundary;
 - (b) Work requiring the qualified person to interact with (e.g., operate, service, maintain, adjust) the equipment when conductors or circuit parts are not exposed but an increased likelihood of injury from an exposure to an arc-flash hazard exists;
 - (c) Work requiring the qualified person to interact with equipment or circuits⁶ that are not known to be properly installed or maintained; or

⁶ These requirements do not apply to plugging equipment into, or unplugging equipment from, receptacles or to operating lights utilizing switch-rated devices.

- (d) Work requiring the qualified person to interact with equipment or circuits⁴ when the upstream protective devices are not known to be properly installed or maintained.

f. [EEWPs](#) (NIST-380 and NIST-380A Forms)

OUs shall authorize permit-required energized electrical work by completing [EEWPs](#) in accordance with the requirements of this section. There are two categories of permit-required energized electrical work:

- Permit-required energized electrical work associated with laboratory and R&D activities covered by OU-approved hazard reviews, as described in Section [6f\(1\)](#); and
- All other permit-required energized electrical work, as described in Section [6f\(2\)](#).

(1) Permit-Required Energized Electrical Work Covered by OU-Approved Hazard Reviews

For permit-required energized electrical work covered by an OU-approved hazard review, the following shall apply:

- (a) The hazard review shall comply with the requirements of [NIST S 7101.20, *Work and Worker Authorization Based on Hazard Reviews*](#).
- (b) The NIST-380A EEWPs short form (see [Appendix H](#)) shall be used to document the following:⁷
- i. Justification for performing the energized work:
 - (i) Why de-energizing the equipment or circuit introduces additional hazards, introduces increased risk, or could cause significant property damage or loss of critical data; or
 - (ii) Why de-energizing the equipment or circuit is infeasible (not just inconvenient) due to equipment design or operational limitations;
 - ii. The hazard analysis of the energized electrical work to be performed;
 - iii. The requestor; and

⁷ The NIST-380A short form contains Sections A (in part), B, C, F, and G of the NIST-380 form. The hazard review must contain all applicable information required by the other sections of the NIST-380 form.

- iv. The approval of the NIST-380A short form by the OSHE Electrical Safety Engineer ([ESE](#)) (see Section 7, Definitions).
- (c) The approved NIST-380A short form shall be appended to the OU-approved hazard review.
- (d) The approved NIST-380A short form and OU-approved hazard review shall be readily available to those performing the energized electrical work.

(2) All Other Permit-Required Energized Electrical Work

For all other permit-required energized electrical work, the NIST-380 EEWP form (see [Appendix I](#)) shall be used to document the following:

- (a) Details of the work to be completed, including:
 - i. The work order associated with the work (if applicable);
 - ii. Location of the work to be performed;
 - iii. Description of the electrical equipment and circuit description;
 - iv. Description of the task;
 - v. The requestor;
 - vi. The qualified person(s) requested to perform the work; and
 - vii. The first-level supervisor(s) of the qualified person(s) requested to perform the work.
- (b) Justification for performing the energized electrical work based upon one of the following circumstances (it is understood that an outage was first requested and denied if applicable):
 - i. Why de-energizing the equipment or circuit introduces additional hazards; introduces increased risk, or could cause significant property damage or loss of critical data, or

- ii. Why de-energizing the equipment or circuit is infeasible (not just inconvenient) due to equipment design or operational limitations.
- (c) The hazard analysis of the energized electrical work to be performed.
- (d) The approval of the NIST-380 form by the OSHE [ESE](#) (see Section 7, Definitions).
- (e) The authorization of the [ESE](#)-approved NIST-380 form by the responsible OU Director or an individual designated by the OU Director to authorize the form on his or her behalf.
- (3) Just prior to the commencement of work, a documented pre-work meeting shall be held by the first-level supervisor or designee with the employee(s) and associate(s) performing the work to review the authorized NIST-380 form, work steps, and job/site/environment specific hazards.
- (4) The authorized NIST-380 form shall be located at the work site for the duration of the work.
- (5) Any general comments or issues encountered during the energized electrical work shall be noted on the authorized NIST-380 form so that appropriate revisions to planning and implementation of future energized electrical work can be made.
- (6) Hard or electronic copies of authorized NIST-380 forms shall be kept by the OUs for a minimum of 1 year from the completion of the work.
- g. Energized Electrical Work Other than Electrical LOTO Performed by Outside Service Providers⁸
 - (1) Outside service providers shall not be permitted to commence energized electrical work other than electrical LOTO on NIST electrical, electronic, or electro-mechanical equipment or circuits until:
 - (a) They have exchanged energized-electrical work programs with the NIST controlling organization; and
 - (b) Arc flash and shock protective boundaries have been established using approved methods to prohibit NIST employees and associates from entering the work area(s).

⁸ Electrical LOTO performed by outside service providers is addressed in NIST S 7101.56: *Control of Hazardous Energy (Lockout/Tagout)* [see Section 6b(1)].

h. Equipment Labeling

(1) Electrical equipment such as switchboards, panelboards, industrial control panels, meter-socket enclosures, motor-control centers, and 3-phase service disconnects shall be field-marked with an electrical-safety label containing all the following information for all new installations and when any modifications, i.e. addition/deletions of components or major repairs, of existing installations are performed:

- (a) Available incident energy;
- (b) Arc flash boundary;
- (c) Working distance;
- (d) Corresponding working distance;
- (e) Nominal system voltage;
- (f) Limited approach boundary;
- (g) Restricted approach boundary;
- (h) Building number;
- (i) Panel number or equipment buss name;
- (j) Upstream protective device panel number/name; and
- (k) Date label issued.

(2) Electrical safety label format shall be as depicted in Appendix J.

i. Training

(1) Employees and associates whose duties require them to be [qualified persons](#) (see Definition 7, Definitions) shall complete:

- (a) The training provided by OSHE on the electrical safe work practices, the scope of which will depend on the nature of the work the qualified person is to perform; and

- (b) The OU-provided activity-specific training on the tasks they perform, including training on the proper use of electrical test equipment, as applicable.
- (2) Employees and associates whose duties require them to be [competent persons](#) (see Definition 7, Definitions) shall:
 - (a) Meet all the requirements of a qualified person; and
 - (b) Be approved by the Authority Having Jurisdiction ([AHJ](#)) as having detailed knowledge regarding the exposure to electrical hazards, the appropriate control methods to reduce the risk associated with those hazards, and the implementation of those methods.
- j. Incident Response
 - (1) Employees and associates who have received electric shocks or been exposed to arc flashes shall immediately receive medical evaluations.
- k. Incident Investigations
 - (1) The OSHE [ESE](#) (or designee) shall be included in investigations of safety incidents involving electric shocks or arc flashes.

6. DEFINITIONS

- a. Authority Having Jurisdiction (AHJ) – The OSHE individual responsible for enforcing the requirements of fire, electrical, and life safety codes and standards at sites owned and operated by NIST, and for approving, as necessary, applicable equipment, materials, installations, and procedures.
- b. Arc Flash – A flashover of electric current through the air from one conductor to another, or to ground.
- c. Arc Flash Boundary – An approach limit at a distance from exposed live parts at which a person could receive a second degree burn if an electrical arc flash were to occur. The boundary is established at the point away from a potential arc source where the incident energy would be reduced to 1.2 cal/cm².
- d. Competent Person – An individual who:

- (1) Meets all the requirements of a qualified person;
 - (2) Is responsible for all work activities or safety procedures related to custom or special equipment used in laboratory or R&D activities; and
 - (3) Has been approved by the AHJ, or by the OSHE ESE as delegated by the AHJ, as having detailed knowledge regarding the exposure to electrical hazards, the appropriate control methods to reduce the risk associated with those hazards, and the implementation of those methods.
- e. De-energized – Free from any electrical connection to a source of potential difference and from electrical charge; not having a potential different from that of the earth.
 - f. Diagnostics – Taking readings or measurements of electrical equipment with approved test equipment that does not require making any physical change to the equipment.
 - g. Electrical Hazard – A dangerous condition such that contact or equipment failure can result in electric shock, arc flash burn, thermal burn, or blast. The limited and restricted approach boundaries (for shock) and the arc flash boundary are the boundaries within which potential electrical hazards to workers exist.
 - h. Electrical Safe Work Condition – A state in which an electrical conductor or circuit part has been disconnected from energized parts, locked/tagged in accordance with established standards, tested to ensure the absence of voltage, and grounded if determined necessary.
 - i. Energized Electrical Work – Work conducted by an employee or associate on electrical, electronic, or electro-mechanical equipment or circuits where:
 - (a) The equipment or circuit is either known to be energized or not known to have been de-energized in accordance with the requirements of this suborder; and
 - (b) The employee or associate is within the restricted-approach boundary or interacts with the equipment or circuit within the arc-flash boundary.
 - j. Energized Electrical Work Analysis and Authorization Permit – A document that details the following:
 - (1) The circuit, equipment, and location of the job/task to be conducted.
 - (2) The work that is to be done.

(3) Justification of why the circuit or equipment cannot be de-energized or the work deferred until the next scheduled outage.

- k. Equipment – A general term, including circuits, components, devices, and the like, used as a part of, or in connection with, an electrical installation.
- l. Exposed (as applied to energized electrical conductors or circuit parts) – Capable of being inadvertently touched or approached nearer than a safe distance by a person. It is applied to electrical conductors or circuit parts that are not suitably guarded, isolated, or insulated.
- m. High Voltage – Voltages above 600 volts.
- n. Incident Energy – The amount of energy impressed on a surface, a certain distance from a source, generated during an electrical arc event. The incident energy level is expressed in calories per centimeter-squared (cal/cm^2) and is a measure of the heat created by the electrical arc.
- o. Laboratory – A building, space, room, or group of rooms intended to serve activities involving procedures for investigation, diagnostics, product testing, or use of custom or special electrical components, systems, or equipment.
- p. Limited Approach Boundary – An approach limit at a distance from an exposed energized electrical conductor or circuit part within which a shock hazard exists.
- q. Low Voltage – Voltages 600 volts and below.
- r. Notice – A temporary directive issued in response to any matter requiring prompt action. Occupational safety and health notices are reviewed annually and automatically renewed unless rescinded by the Chief Safety Officer.
- s. OSHE Electrical Safety Engineer – The individual in OSHE designated by the AHJ to:
 - (1) Approve EEWPs; and
 - (2) Make recommendations to the AHJ on interpretations of the applicable codes/standards, the approval of equipment and materials, and the granting of special permission contemplated in some of the rules.
- t. Properly Installed – Equipment or circuit that has been installed in accordance with applicable industry codes and standards and the manufacturer's recommendations.

- u. Properly Maintained – Equipment or circuit that has been maintained in accordance with applicable industry codes and standards and the manufacturer’s recommendations.
- v. Qualified Person – One who has demonstrated knowledge, skills, and abilities related to the construction, installation, and operation of specific electrical equipment or circuits and has received safety training to identify and avoid the hazards involved.
- w. Repair – Any physical alteration of electrical equipment, e.g., making or tightening connections, removing or replacing components.
- x. Research and Development – An activity in an installation specifically designated for research or development conducted with custom or special electrical equipment.
- y. Restricted Approach Boundary – An approach limit at a distance from an exposed live part within which there is an increased risk of shock, due to electrical arc-over combined with inadvertent movement, for personnel working in close proximity to the live part. This area is reserved only for qualified persons. Shock protection techniques and safety equipment are required.
- z. Suborder – A directive within the NIST Directives Management System that establishes authorities, technical requirements, and assignment of responsibilities in a specific subject area under an order and focuses on the technical details of the program.
- aa. Testing – See definition of “Diagnostics”.
- bb. Work – See definition of “Working On”.
- cc. Working – See definition of “Working On”.
- dd. Working On (Energized Electrical Conductors or Circuit Parts) – Intentionally coming in contact with energized electrical conductors or circuit parts with the hands, feet, or other body parts, with tools, probes, or with test equipment, regardless of the personal protective equipment (PPE) a person is wearing. There are two categories of “working on”: “Diagnostics” (“Testing”) and “Repair” (see definitions).

8. ACRONYMS

- a. ac – Alternating Current
- b. AHJ – Authority Having Jurisdiction.
- c. EEWP – Energized Electrical Work Permit
- d. dc – Direct Current
- e. ESE – Electrical Safety Engineer
- f. LOTO – Lockout/Tagout
- g. NFPA – National Fire Protection Association
- h. OU – Organizational Unit
- i. OSHA – Occupational Safety and Health Administration
- j. OSHE – Office of Safety, Health, and Environment
- k. PPE – Personal Protective Equipment
- l. R&D – Research and Development

9. RESPONSIBILITIES

For responsibilities applicable to all NIST OSH Suborders, see the “Responsibilities” section of [NIST O 7101.00](#).

- a. OU Directors are responsible for:

- (1) Ensuring that the requirements of this notice are met in their respective OUs; and
- (2) Authorizing EEWPs.

- b. OU Line Management is responsible for:

- (1) Authorizing, in accordance with OU procedures, energized electrical work not requiring EEWPs.

- c. Those Responsible for Outside Service Providers Performing Energized Electrical Work are responsible for:
- (1) Ensuring that NIST employees and associates are prohibited access to area(s) in which energized electrical work is taking place until they have been informed of the hazards and of the measures necessary to avoid exposure.
- d. Competent Persons are responsible for:
- (1) The safety of, and safety procedures related to, custom or special equipment associated with laboratory or R&D activities.
- e. OSHE ESE is responsible for:
- (1) Approving EEWPs;
 - (2) Participating in (or designating another individual to participate in) investigations of safety incidents involving electric shocks or arc flashes;
 - (3) Recommending to the AHJ interpretations of the applicable codes/standards, deciding on the approval of equipment and materials, and granting the *special permission* contemplated in some of the rules; and
 - (4) Recommending to the AHJ the approval of individuals as competent persons.
- f. AHJ is responsible for:
- (1) Making interpretations of the applicable codes/standards, deciding on the approval of equipment and materials, and granting the special permission contemplated in some of the rules, i.e., waiving specific requirements in the codes/standards or permitting alternative methods where it is assured that equivalent objectives can be achieved by establishing and maintaining effective safety;
 - (2) Approving individuals as competent persons; and
 - (3) Maintaining a list of competent persons.

10. AUTHORITIES

Authorities common to all NIST OSH suborders can be found in the “Authorities” section of [NIST O 7101.00](#). Authorities specific to this suborder are:

a. OU Directors:

- (1) To delegate to OU Deputy Directors and Division Chiefs (or equivalent) the authority to authorize EEWPs on their behalf.

b. AHJ:

- (1) To delegate to the OSHE ESE the authority to carry out the AHJ responsibilities listed above as they apply to this Notice.

11. DIRECTIVE OWNER

Chief Safety Officer

12. APPENDICES

- A. Revision History
- B. Approach Boundaries to Energized Electrical Conductors or Circuit Parts for Shock Protection for Alternating-Current Systems
- C. Approach Boundaries to Energized Electrical Conductors or Circuit Parts for Shock Protection, Direct-Current Voltage Systems
- D. Arc Flash Hazard Identification Table
- E. Arc-Flash Hazard PPE Categories for Alternating Current (ac) Systems
- F. Arc-Flash Hazard PPE Categories for Direct Current (dc) Systems
- G. PPE Categories
- H. NIST-380A Form: Energized Electrical Work Permit (EEWP) Short Form
- I. NIST-380 Form: Energized Electrical Work Permit (EEWP)

J. Electrical Safety Label Format

Appendix A. Revision History

Revision	Date	Responsible Person	Description of Change
None	10/21/2015	Monroe Charlton	None – Initial document

**Appendix B. Approach Boundaries to Energized Electrical Conductors or Circuit Parts for Shock Protection for Alternating-Current Systems (All dimensions are distance from energized electrical conductor or circuit part to employee).
(2015 NFPA 70E Table 130.4(D)(a))**

(1) Nominal System Voltage Range, Phase to Phase	(2) Limited Approach Boundaries		(4) Restricted Approach Boundary; Includes Inadvertent Movement Adder
	Exposed Movable Conductor	Exposed Fixed Circuit Part	
<50 V	Not specified	Not specified	Not specified
50 V–150 V	3.0 m (10 ft 0 in.)	1.0 m (3 ft 6 in.)	Avoid contact
151 V–750 V	3.0 m (10 ft 0 in.)	1.0 m (3 ft 6 in.)	0.3 m (1 ft 0 in.)
751 V–15 kV	3.0 m (10 ft 0 in.)	1.5 m (5 ft 0 in.)	0.7 m (2 ft 2 in.)
15.1 kV–36 kV	3.0 m (10 ft 0 in.)	1.8 m (6 ft 0 in.)	0.8 m (2 ft 7 in.)
36.1 kV–46 kV	3.0 m (10 ft 0 in.)	2.5 m (8 ft 0 in.)	0.8 m (2 ft 9 in.)
46.1 kV–72.5 kV	3.0 m (10 ft 0 in.)	2.5 m (8 ft 0 in.)	1.0 m (3 ft 3 in.)
72.6 kV–121 kV	3.3 m (10 ft 8 in.)	2.5 m (8 ft 0 in.)	1.0 m (3 ft 4 in.)
138 kV–145 kV	3.4 m (11 ft 0 in.)	3.0 m (10 ft 0 in.)	1.2 m (3 ft 10 in.)
161 kV–169 kV	3.6 m (11 ft 8 in.)	3.6 m (11 ft 8 in.)	1.3 m (4 ft 3 in.)
230 kV–242 kV	4.0 m (13 ft 0 in.)	4.0 m (13 ft 0 in.)	1.7 m (5 ft 8 in.)
345 kV–362 kV	4.7 m (15 ft 4 in.)	4.7 m (15 ft 4 in.)	2.8 m (9 ft 2 in.)
500 kV–550 kV	5.8 m (19 ft 0 in.)	5.8 m (19 ft 0 in.)	3.6 m (11 ft 10 in.)
765 kV–800 kV	7.2 m (23 ft 9 in.)	7.2 m (23 ft 9 in.)	4.9 m (15 ft 11 in.)

Note (1): For arc flash boundary, see 130.5(A).

Note (2): All dimensions are distance from exposed energized electrical conductors or circuit part to employee.

a For single-phase systems above 250V, select the range that is equal to the system's maximum phase-to-ground voltage multiplied by 1.732.

b See definition in Article 100 and text in 130.4(D)(2) and Informative Annex C for elaboration.

c *Exposed movable conductors* describes a condition in which the distance between the conductor and a person is not under the control of the person. The term is normally applied to overhead line conductors supported by poles.

d This includes circuits where the exposure does not exceed 120V.

**Appendix C. Approach Boundaries to Energized Electrical Conductors or Circuit Parts for
Shock Protection, Direct-Current Voltage Systems
(2015 NFPA 70E Table 130.4(D)(b))**

(1) Nominal Potential Difference	(2) Limited Approach Boundaries		(4) Restricted Approach Boundary; Includes Inadvertent Movement Adder
	Exposed Movable Conductor	Exposed Fixed Circuit Part	
<100 V	Not specified	Not specified	Not specified
100 V–300 V	3.0 m (10 ft 0 in.)	1.0 m (3 ft 6 in.)	Avoid contact
301 V–1 kV	3.0 m (10 ft 0 in.)	1.0 m (3 ft 6 in.)	0.3 m (1 ft 0 in.)
1.1 kV–5 kV	3.0 m (10 ft 0 in.)	1.5 m (5 ft 0 in.)	0.5 m (1 ft 5 in.)
5 kV–15 kV	3.0 m (10 ft 0 in.)	1.5 m (5 ft 0 in.)	0.7 m (2 ft 2 in.)
15.1 kV–45 kV	3.0 m (10 ft 0 in.)	2.5 m (8 ft 0 in.)	0.8 m (2 ft 9 in.)
45.1 kV– 75 kV	3.0 m (10 ft 0 in.)	2.5 m (8 ft 0 in.)	1.0 m (3 ft 2 in.)
75.1 kV–150 kV	3.3 m (10 ft 8 in.)	3.0 m (10 ft 0 in.)	1.2 m (4 ft 0 in.)
150.1 kV–250 kV	3.6 m (11 ft 8 in.)	3.6 m (11 ft 8 in.)	1.6 m (5 ft 3 in.)
250.1 kV–500 kV	6.0 m (20 ft 0 in.)	6.0 m (20 ft 0 in.)	3.5 m (11 ft 6 in.)
500.1 kV–800 kV	8.0 m (26 ft 0 in.)	8.0 m (26 ft 0 in.)	5.0 m (16 ft 5 in.)

Note: All dimensions are distance from exposed energized electrical conductors or circuit parts to worker.

* Exposed movable conductor describes a condition in which the distance between the conductor and a person is not under the control of the person. The term is normally applied to overhead line conductors supported by poles.

**Appendix D. Arc Flash Hazard Identification Table
(2015 NFPA 70E Table 130.7(C)(15)(A)(a))**

Task	Equipment Condition*	Arc Flash PPE Required
Reading a panel meter while operating a meter switch	Any	No
Normal operation of a circuit breaker (CB), switch, contactor, or starter	<p>All of the following:</p> <p>The equipment is properly installed The equipment is properly maintained All equipment doors are closed and secured All equipment covers are in place and secured There is no evidence of impending failure</p>	No
	<p>One or more of the following:</p> <p>The equipment is not properly installed The equipment is not properly maintained Equipment doors are open or not secured Equipment covers are off or not secured There is evidence of impending failure</p>	Yes
For ac systems: Work on energized electrical conductors and circuit parts, including voltage testing	Any	Yes
For dc systems: Work on energized electrical conductors and circuit parts of series-connected battery cells, including voltage testing	Any	Yes
Voltage testing on individual battery cells or individual multi-cell units	<p>All of the following:</p> <p>The equipment is properly installed The equipment is properly maintained Covers for all other equipment are in place and secured There is no evidence of impending failure</p>	No
	<p>One or more of the following:</p> <p>The equipment is not properly installed The equipment is not properly maintained Equipment doors are open or not secured Equipment covers are off or not secured There is evidence of impending failure</p>	Yes
Removal or installation of CBs or switches	Any	Yes

**Appendix D. Arc Flash Hazard Identification Table
(2015 NFPA 70E Table 130.7(C)(15)(A)(a))**

Task	Equipment Condition*	Arc Flash PPE Required
Removal or installation of covers for equipment such as wireways, junction boxes, and cable trays that does not expose bare energized electrical conductors and circuit parts	<p>All of the following:</p> <p>The equipment is properly installed The equipment is properly maintained There is no evidence of impending failure</p>	No
	<p>Any of the following:</p> <p>The equipment is not properly installed The equipment is not properly maintained There is evidence of impending failure</p>	Yes
Removal of bolted covers (to expose bare energized electrical conductors and circuit parts). For dc systems, this includes bolted covers, such as battery terminal covers.	Any	Yes
Removal of battery intercell connector covers	<p>All of the following:</p> <p>The equipment is properly installed. The equipment is properly maintained Covers for all other equipment are in place and secured There is no evidence of impending failure</p>	No
	<p>One or more of the following:</p> <p>The equipment is not properly installed The equipment is not properly maintained Equipment doors are open or not secured Equipment covers are off or not secured There is evidence of impending failure</p>	Yes

**Appendix D. Arc Flash Hazard Identification Table
(2015 NFPA 70E Table 130.7(C)(15)(A)(a))**

Task	Equipment Condition*	Arc Flash PPE Required
Opening hinged door(s) or cover(s) (to expose bare energized electrical conductors and circuit parts)	Any	Yes
Perform infrared thermography and other noncontact inspections outside the restricted approach boundary. This activity does not include opening of doors or covers.	Any	No
Application of temporary protective grounding equipment after voltage test	Any	Yes
Work on control circuits with exposed energized electrical conductors and circuit parts, 120 volts or below without any other exposed energized equipment over 120 V including opening of hinged covers to gain access	Any	No
Work on control circuits with exposed energized electrical conductors and circuit parts, greater than 120 V	Any	Yes
Insertion or removal of individual starter buckets from motor control center (MCC)	Any	Yes
Insertion or removal (racking) of CBs or starters from cubicles, doors open or closed	Any	Yes
Insertion or removal of plug-in devices into or from busways	Any	Yes
Insulated cable examination with no manipulation of cable	Any	No
Insulated cable examination with manipulation of cable	Any	Yes
Work on exposed energized electrical conductors and circuit parts of equipment directly supplied by a panelboard or motor control center	Any	Yes
Insertion and removal of revenue meters (kW-hour, at primary voltage and current)	Any	Yes
For dc systems, insertion or removal of individual cells or multi-cell units of a battery system in an enclosure	Any	Yes

**Appendix D. Arc Flash Hazard Identification Table
(2015 NFPA 70E Table 130.7(C)(15)(A)(a))**

Task	Equipment Condition*	Arc Flash PPE Required
For dc systems, insertion or removal of individual cells or multi-cell units of a battery system in an open rack	Any	No
For dc systems, maintenance on a single cell of a battery system or multi-cell units in an open rack	Any	No
For dc systems, work on exposed energized electrical conductors and circuit parts of utilization equipment directly supplied by a dc source	Any	Yes
Arc-resistant switchgear Type 1 or 2 (for clearing times of <0.5 sec with a prospective fault current not to exceed the arc-resistant rating of the equipment) and metal enclosed interrupter switchgear, fused or unfused of arc resistant type construction, tested in accordance with IEEE C37.20.7: •Insertion or removal (racking) of CBs from cubicles •Insertion or removal (racking) of ground and test device •Insertion or removal (racking) of voltage transformers on or off the bus	All of the following: The equipment is properly installed The equipment is properly maintained All equipment doors are closed and secured All equipment covers are in place and secured There is no evidence of impending failure	No
	One or more of the following: The equipment is not properly installed The equipment is not properly maintained Equipment doors are open or not secured Equipment covers are off or not secured There is evidence of impending failure	Yes
Opening voltage transformer or control power transformer compartments	Any	Yes
Outdoor disconnect switch operation (hookstick operated) at 1 kV through 15 kV	Any	Yes
Outdoor disconnect switch operation (gang-operated, from grade) at 1 kV through 15 kV	Any	Yes

Note: Hazard identification is one component of risk assessment. Risk assessment involves a determination of the likelihood of occurrence of an incident, resulting from a hazard that could cause injury or damage to health. The assessment of the likelihood of occurrence contained in this table does not cover every possible condition or situation. Where this table indicates that arc flash PPE is not required, an arc flash is not likely to occur

**Appendix E. Arc-Flash Hazard PPE Categories for Alternating Current (ac) Systems
(2015 NFPA 70E Table 130.7(C)(15)(B))**

Equipment	Arc Flash PPE Category	Arc-Flash Boundary
Panelboards or other equipment rated 240 V and below Parameters: Maximum of 25 kA short-circuit current available; maximum of 0.03 sec (2 cycles) fault clearing time; working distance 455 mm (18 in.)	1	485 mm (19 in.)
Panelboards or other equipment rated >240 V and up to 600 V Parameters: Maximum of 25 kA short-circuit current available; maximum of 0.03 sec (2 cycles) fault clearing time; working distance 455 mm (18 in.)	2	900 mm (3 ft)
600-V class motor control centers (MCCs) Parameters: Maximum of 65 kA short-circuit current available; maximum of 0.03 sec (2 cycles) fault clearing time; working distance 455 mm (18 in.)	2	1.5 m (5 ft)
600-V class motor control centers (MCCs) Parameters: Maximum of 42 kA short-circuit current available; maximum of 0.33 sec (20 cycles) fault clearing time; working distance 455 mm (18 in.)	4	4.3 m (14 ft)
600-V class switchgear (with power circuit breakers or fused switches) and 600 V class switchboards Parameters: Maximum of 35 kA short-circuit current available; maximum of up to 0.5 sec (30 cycles) fault clearing time; working distance 455 mm (18 in.)	4	6 m (20 ft)
Other 600-V class (277 V through 600 V, nominal) equipment Parameters: Maximum of 65 kA short circuit current available; maximum of 0.03 sec (2 cycles) fault clearing time; working distance 455 mm (18 in.)	2	1.5 m (5 ft)
NEMA E2 (fused contactor) motor starters, 2.3 kV through 7.2 kV Parameters: Maximum of 35 kA short-circuit current available; maximum of up to 0.24 sec (15 cycles) fault clearing time; working distance 910 mm (36 in.)	4	12 m (40 ft)
Metal-clad switchgear, 1 kV through 15 kV Parameters: Maximum of 35 kA short-circuit current available; maximum of up to 0.24 sec (15 cycles) fault clearing time; working distance 910 mm (36 in.)	4	12 m (40 ft)
Arc-resistant switchgear Type 1 or 2 [for clearing times of < 0.5 sec (30 cycles) with a perspective fault current not to exceed the arc-resistant rating of the equipment], and metal-enclosed interrupter switchgear, fused or unfused of arc-resistant-type construction, tested in accordance with IEEE C37.20.7, 1 kV through 15 kV Parameters: Maximum of 35 kA short-circuit current available; maximum of up to 0.24 sec (15 cycles) fault clearing time; working distance 910 mm (36 in.)	N/A (doors closed)	N/A (doors closed)
	4 (doors open)	12 m (40 ft)
Other equipment 1 kV through 15 kV Parameters: Maximum of 35 kA short-circuit current available; maximum of up to 0.24 sec (15 cycles) fault clearing time; working distance 910 mm (36 in.)	4	12 m (40 ft)

**Appendix F. Arc-Flash Hazard PPE Categories for Direct Current (dc) Systems
(2015 NFPA 70E Table 130.7(C)(15)(B))**

Equipment	Arc Flash PPE Category	Arc-Flash Boundary
Storage batteries, dc switchboards, and other dc supply sources 100 V > Voltage < 250 V Parameters: Voltage: 250 V Maximum arc duration and working distance: 2 sec @ 455 mm (18 in.)		
Short-circuit current < 4 kA	1	900 mm (3 ft)
4 kA ≤ short-circuit current < 7 kA	2	1.2 m (4 ft)
7 kA ≤ short-circuit current < 15 kA	3	1.8 m (6 ft)
Storage batteries, dc switchboards, and other dc supply sources 250 V ≤ Voltage ≤ 600 V Parameters: Voltage: 600 V Maximum arc duration and working distance: 2 sec @ 455 mm (18 in.)		
Short-circuit current 1.5 kA	1	900 mm (3 ft)
1.5 kA ≤ short-circuit current < 3 kA	2	1.2 m (4 ft)
3 kA ≤ short-circuit current < 7 kA	3	1.8 m (6 ft.)
7 kA ≤ short-circuit current < 10 kA	4	2.5 m (8 ft)

Note: Apparel that can be expected to be exposed to electrolyte must meet both of the following conditions:

- (1) Be evaluated for electrolyte protection in accordance with ASTM F1296, *Standard Guide for Evaluating Chemical Protective Clothing*
- (2) Be arc-rated in accordance with ASTM F1891, *Standard Specification for Arc Rated and Flame Resistant Rainwear*, or equivalent

Appendix G. Table 130.7(C)(16) Personal Protective Equipment (PPE)

PPE Category	PPE
1	Arc-Rated Clothing, Minimum Arc Rating of 4 cal/cm ² (see Note 1)
	Arc-rated long-sleeve shirt and pants or arc-rated coverall
	Arc-rated face shield (see Note 2) or arc flash suit hood
	Arc-rated jacket, parka, rainwear, or hard hat liner (AN)
	Protective Equipment
	Hard hat
	Safety glasses or safety goggles (SR)
	Hearing protection (ear canal inserts)
	Heavy duty leather gloves (see Note 3)
	Leather footwear (AN)
2	Arc-Rated Clothing, Minimum Arc Rating of 8 cal/cm ² (see Note 1)
	Arc-rated long-sleeve shirt and pants or arc-rated coverall
	Arc-rated flash suit hood or arc-rated face shield (see Note 2) and arc-rated balaclava
	Arc-rated jacket, parka, rainwear, or hard hat liner (AN)
	Protective Equipment
	Hard hat
	Safety glasses or safety goggles (SR)
	Hearing protection (ear canal inserts)
	Heavy duty leather gloves (see Note 3)
	Leather footwear
3	Arc-Rated Clothing Selected so That the System Arc Rating Meets the Required Minimum Arc Rating of 25 cal/cm ² (see Note 1)
	Arc-rated long-sleeve shirt (AR)
	Arc-rated pants (AR)
	Arc-rated coverall (AR)
	Arc-rated arc flash suit jacket (AR)
	Arc-rated arc flash suit pants (AR)
	Arc-rated arc flash suit hood
	Arc-rated gloves (see Note 1)
	Arc-rated jacket, parka, rainwear, or hard hat liner (AN)
	Protective Equipment
	Hard hat
	Safety glasses or safety goggles (SR)
	Hearing protection (ear canal inserts)
	Leather footwear
4	Arc-Rated Clothing Selected so That the System Arc Rating Meets the Required Minimum Arc Rating of 40 cal/cm ² (see Note 1)
	Arc-rated long-sleeve shirt (AR)
	Arc-rated pants (AR)
	Arc-rated coverall (AR)

Appendix G. Table 130.7(C)(16) Personal Protective Equipment (PPE)

	Arc-rated arc flash suit jacket (AR)
	Arc-rated arc flash suit pants (AR)
	Arc-rated arc flash suit hood
	Arc-rated gloves (see Note 1)
	Arc-rated jacket, parka, rainwear, or hard hat liner (AN)
	Protective Equipment
	Hard hat
	Safety glasses or safety goggles (SR)
	Hearing protection (ear canal inserts)
	Leather footwear
	AN: as needed (optional). AR: as required. SR: selection required.
Notes:	(1) <i>Arc rating</i> is defined in Article 100.
	(2) Face shields are to have wrap-around guarding to protect not only the face but also the forehead, ears, and neck, or, alternatively, an arc-rated arc flash suit hood is required to be worn.
	(3) If rubber insulating gloves with leather protectors are used, additional leather or arc-rated gloves are not required. The combination of rubber insulating gloves with leather protectors satisfies the arc flash protection requirement.

Appendix H. NIST-380A: Energized Electrical Work Permit (EEWP) Short Form

NIST-380A (9-2015) NFPA 70E Article 130.2(B)		U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	
ENERGIZED ELECTRICAL WORK PERMIT SHORT FORM			
A. WORK ORDER DETAIL			
Work Order Number	Building Number	Location/Area	Date of Request
Electrical Equipment and/or Circuit Description			
Task Description			
B. JUSTIFICATION FOR ENERGIZED WORK			
<input type="checkbox"/> De-energizing the equipment or circuit introduces additional hazards; introduces increased risk, or could cause significant property damage or loss of critical data Explain:			
<input type="checkbox"/> De-energizing the equipment or circuit is infeasible (not just inconvenient) due to equipment design or operational limitations Explain:			
<input type="checkbox"/> An outage was requested and denied			
Printed Name/Title		Signature/Date	
C. REQUESTOR			
Name & Title (Print)		(Signature)	
D. QUALIFIED PERSON			
Name & Title (Print)		(Signature)	
E. REQUESTOR SUPERVISOR/MANAGER			
Name & Title (Print)		(Signature)	
NIST-380A (9-2015)		Total Number of Pages ____	

Appendix H. NIST-380A: Energized Electrical Work Permit (EERP) Short Form

ENERGIZED ELECTRICAL WORK PERMIT SHORT FORM														
F. HAZARD ANALYSIS (SECTION REQUIRED FOR BOTH ON OR NEAR EXPOSED ENERGIZED PARTS)														
1. Maximum exposure in Volts _____ Maximum Amperage kA _____ Fault Clear Time _____ (cycles)														
2. Energized Exposure Hazard: Working on or near: <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> Bare Bus</td> <td><input type="checkbox"/> Open Terminals</td> <td><input type="checkbox"/> NEMA E2 Motor Starters</td> </tr> <tr> <td><input type="checkbox"/> Bare conductor</td> <td><input type="checkbox"/> Panel boards</td> <td><input type="checkbox"/> Metal Clad Switch gear</td> </tr> <tr> <td><input type="checkbox"/> Open circuit(s)</td> <td><input type="checkbox"/> Switch boards</td> <td><input type="checkbox"/> Confined Space</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> Energized Feeders</td> <td>List: _____</td> </tr> </table>			<input type="checkbox"/> Bare Bus	<input type="checkbox"/> Open Terminals	<input type="checkbox"/> NEMA E2 Motor Starters	<input type="checkbox"/> Bare conductor	<input type="checkbox"/> Panel boards	<input type="checkbox"/> Metal Clad Switch gear	<input type="checkbox"/> Open circuit(s)	<input type="checkbox"/> Switch boards	<input type="checkbox"/> Confined Space	<input type="checkbox"/> Energized Feeders		List: _____
<input type="checkbox"/> Bare Bus	<input type="checkbox"/> Open Terminals	<input type="checkbox"/> NEMA E2 Motor Starters												
<input type="checkbox"/> Bare conductor	<input type="checkbox"/> Panel boards	<input type="checkbox"/> Metal Clad Switch gear												
<input type="checkbox"/> Open circuit(s)	<input type="checkbox"/> Switch boards	<input type="checkbox"/> Confined Space												
<input type="checkbox"/> Energized Feeders		List: _____												
Other (List): _____														
3. Method of analysis: NFPA 70E Tables <input type="checkbox"/> Calculations <input type="checkbox"/>														
4. Shock Hazard Analysis: Limited Approach Boundary _____ ft _____ in Restricted Approach Boundary _____ ft _____ in														
5. Flash Hazard Analysis: Flash Protection Boundary _____ ft _____ in Incident Energy Value _____ cal/cm ² at _____ ft _____ in Working Distance														
6. PPE Category: 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/>														
7. PPE Minimum FR Rating: _____ cal/cm ²														
8. Required PPE & Tools: <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> V Rated Gloves</td> <td><input type="checkbox"/> V Rated Tools</td> <td><input type="checkbox"/> Face Shield</td> <td><input type="checkbox"/> Leather Shoes</td> </tr> <tr> <td><input type="checkbox"/> FR Shirt</td> <td><input type="checkbox"/> FR Pants</td> <td><input type="checkbox"/> Leather Gloves</td> <td><input type="checkbox"/> Flash Suit</td> </tr> <tr> <td><input type="checkbox"/> Hard Hat</td> <td><input type="checkbox"/> Hearing Protection (Ear Plugs, Muffs or Both)</td> <td><input type="checkbox"/> Coveralls</td> <td><input type="checkbox"/> Flash Hood</td> </tr> </table>			<input type="checkbox"/> V Rated Gloves	<input type="checkbox"/> V Rated Tools	<input type="checkbox"/> Face Shield	<input type="checkbox"/> Leather Shoes	<input type="checkbox"/> FR Shirt	<input type="checkbox"/> FR Pants	<input type="checkbox"/> Leather Gloves	<input type="checkbox"/> Flash Suit	<input type="checkbox"/> Hard Hat	<input type="checkbox"/> Hearing Protection (Ear Plugs, Muffs or Both)	<input type="checkbox"/> Coveralls	<input type="checkbox"/> Flash Hood
<input type="checkbox"/> V Rated Gloves	<input type="checkbox"/> V Rated Tools	<input type="checkbox"/> Face Shield	<input type="checkbox"/> Leather Shoes											
<input type="checkbox"/> FR Shirt	<input type="checkbox"/> FR Pants	<input type="checkbox"/> Leather Gloves	<input type="checkbox"/> Flash Suit											
<input type="checkbox"/> Hard Hat	<input type="checkbox"/> Hearing Protection (Ear Plugs, Muffs or Both)	<input type="checkbox"/> Coveralls	<input type="checkbox"/> Flash Hood											
9. Is work required to be performed in area classified as a "Confined Space"? Yes <input type="checkbox"/> No <input type="checkbox"/>														
10. If manhole work, can the work be performed at least 18" from energized cables or splices? Yes <input type="checkbox"/> No <input type="checkbox"/>														
11. Engineering/Administrative Controls Planned to Reduce/Eliminate Exposure to Energized Equipment: Put Protective Relays in Maintenance Settings <input type="checkbox"/> <table style="width: 100%; border: none;"> <tr> <td>Insulating Blankets <input type="checkbox"/></td> <td>If checked, provide details below or on an attached diagram (required)</td> </tr> <tr> <td>Arc Suppression Blankets <input type="checkbox"/></td> <td>If checked, provide details below or on an attached diagram (required)</td> </tr> <tr> <td>Other Controls <input type="checkbox"/></td> <td>If checked, provide details below or on an attached diagram (required)</td> </tr> </table>			Insulating Blankets <input type="checkbox"/>	If checked, provide details below or on an attached diagram (required)	Arc Suppression Blankets <input type="checkbox"/>	If checked, provide details below or on an attached diagram (required)	Other Controls <input type="checkbox"/>	If checked, provide details below or on an attached diagram (required)						
Insulating Blankets <input type="checkbox"/>	If checked, provide details below or on an attached diagram (required)													
Arc Suppression Blankets <input type="checkbox"/>	If checked, provide details below or on an attached diagram (required)													
Other Controls <input type="checkbox"/>	If checked, provide details below or on an attached diagram (required)													
12. Additional controls/comments/means to restrict access														
13. Engineering Hazard Analysis completed by: <table style="width: 100%; border: none; margin-top: 20px;"> <tr> <td style="width: 33%; text-align: center;">_____</td> <td style="width: 33%; text-align: center;">_____</td> <td style="width: 33%; text-align: center;">_____</td> </tr> <tr> <td style="text-align: center;">PRINTED NAME</td> <td style="text-align: center;">SIGNATURE</td> <td style="text-align: center;">DATE</td> </tr> </table>			_____	_____	_____	PRINTED NAME	SIGNATURE	DATE						
_____	_____	_____												
PRINTED NAME	SIGNATURE	DATE												

Appendix H. NIST-380A: Energized Electrical Work Permit (EEWP) Short Form

[illegible]

Appendix I. NIST-380: Energized Electrical Work Permit (EEWP)

NIST-380 (9-2015) NFPA 70E Article 130.2(B)		U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	
ENERGIZED ELECTRICAL WORK PERMIT			
A. WORK ORDER DETAIL			
Work Order Number	Building Number	Building/Area	Date of Request
Electrical Equipment and/or Circuit Description <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>			
Task Description: <div style="border: 1px solid black; height: 80px; margin-top: 5px;"></div>			
B. JUSTIFICATION FOR ENERGIZED WORK			
<input type="checkbox"/> De-energizing the equipment or circuit introduces additional hazards; introduces increased risk, or could cause significant property damage or loss of critical data Explain: <div style="border: 1px solid black; height: 100px; margin-top: 5px;"></div>			
<input type="checkbox"/> De-energizing the equipment or circuit is infeasible (not just inconvenient) due to equipment design or operational limitations Explain: <div style="border: 1px solid black; height: 100px; margin-top: 5px;"></div>			
<input type="checkbox"/> An outage was requested and denied Printed Name/Title: _____ Signature/Date: _____			
C. REQUESTOR			
Name & Title (Print)		(Signature)	
D. QUALIFIED PERSON			
Name & Title (Print)		(Signature)	
E. REQUESTOR SUPERVISOR/MANAGER			
Name & Title (Print)		(Signature)	
NIST-380 (9-2015)		Total Number of Pages _____	

ENERGIZED ELECTRICAL WORK PERMIT

1. Maximum exposure in Volts _____ Maximum Amperage kA _____ Fault Clear Time _____ (cycles)


Working on or near:


- Other (*List*):

DATE _____

ENERGIZED ELECTRICAL WORK PERMIT		
G. OSHE ELECTRICAL SAFETY ENGINEER (ESE) OR DESIGNATED REPRESENTATIVE REVIEW & APPROVAL		
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved		
Name & Title (Print)	(Signature)	Date
Comments:		
H. ENERGIZED ELECTRICAL WORK PERMIT AUTHORIZATION		
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved		
OU DIRECTOR or DESIGNATED REPRESENTATIVE / TITLE (Print)	(Signature)	Date
Comments:		
I. ATTACHMENTS		
<u>Number</u>	<u>Pages</u>	<u>Attachment Title</u>
J. NOTES		

Appendix J. Electrical Safety Label Format

 WARNING	
ARC FLASH & SHOCK HAZARD Incident Energy at Working Distance < > Cal/cm ²	
<Enter> Inches	ARC FLASH BOUNDARY
<Enter> Inches	Working Distance
<Enter> Vac	Shock Hazard When Cover Off
<Enter>	Limited Approach Boundary
<Enter >	Restricted Approach Boundary
Building: <Enter > Equip. Buss Name: <Enter >	
Prot. Device: <Enter > Date issued: <Enter >	

 DANGER	
ARC FLASH & SHOCK HAZARD Incident Energy at Working Distance < > Cal/cm ²	
<Enter> Inches	ARC FLASH BOUNDARY
<Enter> Inches	Working Distance
<Enter> Vac	Shock Hazard When Cover Off
<Enter>	Limited Approach Boundary
<Enter >	Restricted Approach Boundary
Building: <Enter > Equip. Buss Name: <Enter >	
Prot. Device: <Enter > Date issued: <Enter >	

Ionizing Radiation Safety

NIST P 7200.00
Effective Date: 9/5/2012

PURPOSE

To augment NIST Policy 710.01, Occupational Safety and Health, by articulating NIST's commitment to ensuring the safe, regulatorily compliant, and responsible use of ionizing radiation by NIST employees and associates.

SCOPE

This policy applies to all activities conducted by NIST employees and associates involving the use of ionizing radiation.

LEGAL AUTHORITY AND REFERENCES

- [Atomic Energy Act, 42 U.S.C. § 2011 et seq.](#)
- [Clean Air Act, as amended, 42 U.S.C. §7401 et seq.](#)
- [Title 10, Code of Federal Regulations, Parts 30, 31, 32, 33, and 36](#)
- [6 Colorado Code of Regulations 1007-1, Radiation Control](#)
- [Title 29, Code of Federal Regulations § 1910.1096, Ionizing Radiation](#)
- [Department of Commerce Department Organization Order 30-2A, National Institute of Standards and Technology](#)

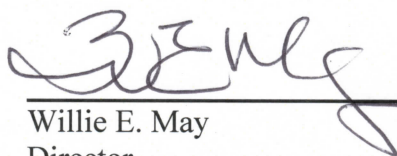
POLICY

Ionizing radiation regulatory requirements in the U.S. require implementation of sound radiation protection principles to keep exposures to individuals, including members of the public, As Low As is Reasonably Achievable (ALARA). The U.S. Nuclear Regulatory Commission defines ALARA as “making every reasonable effort to maintain exposures to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken.” Therefore, it is NIST policy that all NIST activities using ionizing radiation be conducted in a manner consistent with ALARA and compliant with all applicable regulations and other requirements.

The Associate Director for Laboratory Programs shall ensure the development of other directives necessary for the full and effective implementation of this policy as it pertains to the reactor facility at the NIST Center for Neutron Research (NCNR). The development and review of

additional directives covering activities conducted under the reactor license shall be performed in consultation with the NCNR Director.

The Associate Director for Management Resources shall ensure the development of other directives necessary for the full and effective implementation of this policy as it pertains to all other sources of ionizing radiation at NIST.

 7/24/15
Willie E. May Date
Director

Ionizing Radiation Safety – Radioactive Material and Ionizing-Radiation-Producing Machines

NIST O 7201

Document Date: 01/15/2014

Issue Date: 01/15/2014

Effective Date: 01/15/2014

PURPOSE

The purpose of this directive is to define the requirements, roles, responsibilities, and authorities necessary for the full and effective implementation of NIST Policy 720 (NIST P 720), Ionizing Radiation Safety, as it applies to radioactive material and ionizing-radiation-producing machines.

BACKGROUND

Ionizing radiation regulatory requirements in the U.S. require implementation of sound radiation protection principles to keep exposures to individuals, including members of the public, As Low As is Reasonably Achievable (ALARA). It is NIST policy that all NIST activities using ionizing radiation be conducted in a manner consistent with ALARA and compliant with all applicable regulations and other requirements.

APPLICABILITY

This directive applies to on- and off-site activities conducted by NIST employees and associates¹ under the auspices of any Nuclear Regulatory Commission (NRC) radioactive materials license issued to NIST and to the on-site use by NIST employees and associates of ionizing-radiation-producing machines. This directive does not apply to activities conducted under the auspices of the NRC reactor license.

REFERENCES

- [NIST Policy 7200, Ionizing Radiation Safety](#)
- [Title 10, Code of Federal Regulations \(CFR\): Nuclear Regulatory Commission](#)
- [NIST Ionizing Radiation Safety Committee \(IRSC\) Charter](#)

REQUIREMENTS

- In planning work, methods and means to achieve ALARA, such as use of engineering and administrative controls and personal protective equipment, shall be identified and integrated into the conduct of the work

¹ Associates who have entered into agreements with NIST that commit them to complying with NIST's and their sponsoring OU's administrative requirements, including safety requirements.

- Pertinent activities affecting potential exposures of workers and the public and environmental releases shall be evaluated, tracked, and reviewed regularly to determine adherence to ALARA and good practice principles
- Training needed to meet the goals of ALARA and meeting regulatory requirements shall be provided to those with roles and responsibilities related to ionizing radiation safety
- NIST's ionizing-radiation-safety programs shall be reviewed for adherence to ALARA concepts and for general program functionality
- Written procedures shall be developed and implemented to ensure that all applicable regulations and other requirements are met

DEFINITIONS

As Low As is Reasonably Achievable (ALARA) – An acronym for "As Low As is Reasonably Achievable", which means making every reasonable effort to maintain exposures to radiation as far below NRC dose limits in 10 CFR 20 as is practical consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, the economics of improvements in relation to state of technology, the economics of improvements in relation to benefits to the public health and safety, and other societal and socioeconomic considerations, and in relation to utilization of nuclear energy and licensed materials in the public interest. (*See* 10 CFR 20.1003)

Deployment Tools – Tools, such as procedures, forms, instructions, information technology (IT) applications, training, and user guides developed by the Radiation Safety Officers (RSOs) to facilitate the implementation of ionizing radiation safety directives.

Implement – To ensure that the applicable requirements are met.

Ionizing Radiation – Alpha particles, beta particles, gamma rays, x rays, neutrons, high-energy electrons, high-energy protons, and other particles capable of producing ions when they impinge on, or penetrate, matter, hereinafter referred to as "radiation".

Ionizing-Radiation-Producing Machines – Machines that generate ionizing radiation when energized, including, but not limited to, x-ray units, particle accelerators, neutron generators, and electron microscopes.

Ionizing-Radiation-Safety Program – For a set of ionizing-radiation-safety activities of defined scope,² the following elements:³ a suborder; all supporting suborder-specific directives, including procedures, guidance, and notices; all required deployment tools, including training, forms,

² Examples of such sets of activities include those involving radioactive material at NIST Gaithersburg, radioactive material at NIST Boulder ionizing-radiation-producing machines at NIST Gaithersburg, or ionizing-radiation-producing machines at NIST Boulder.

³ To implement a RSP means to ensure that the requirements of this order and the requirements applicable to the set of ionizing radiation-safety activities of defined scope are met.

instructions, and information technology applications; and all written Organizational Unit (OU) procedures required by the suborder or any supporting suborder-specific directive.

Ionizing Radiation Sources (or Sources of Ionizing Radiation) – Radioactive material and ionizing-radiation-producing machines.

Radioactive Material – Material that emits ionizing radiation.

ACRONYMS

ADLP – Associate Director for Laboratory Programs

ADMR – Associate Director for Management Resources

ALARA – As Low As is Reasonably Achievable

CFR – Code of Federal Regulations

CSO – Chief Safety Officer

IRSC – Ionizing Radiation Safety Committee

NIST – National Institute of Standards and Technology

NRC – Nuclear Regulatory Commission

OU – Organizational Unit

RSO – Radiation Safety Officer

ROLES AND RESPONSIBILITIES

NIST Director

- Ensure the implementation and maintenance of effective ionizing-radiation-safety programs at NIST
- Ensure proper allocation of resources for ionizing radiation safety at NIST
- Ensures that individuals are held accountable for meeting NIST's radiation-safety-program requirements
- Provide direction on issues involving ionizing radiation safety and regulatory and license compliance
- Provide direction to the Associate Director for Laboratory Programs (ADLP), Associate Director for Management Resources (ADMR), Chief Safety Officer (CSO), RSOs, IRSC, and OU Directors, as necessary
- Approve the IRSC charter and changes thereto, subject to NRC license requirements
- Appoint all IRSC members, subject to NRC license requirements
- Review IRSC recommendations and direct action on those recommendations as necessary

NIST Associate Directors

- Support the NIST Director in carrying out his or her responsibilities
- Ensure the implementation of NIST's ionizing-radiation-safety programs in their respective directorates
- Ensure proper allocation of resources for ionizing radiation safety in their respective directorates
- Ensure that individuals are held accountable for meeting NIST's radiation-safety-program requirements in their respective directorates
- Provide direction as needed on issues involving ionizing radiation safety and regulatory and license compliance within their respective directorates
- Review the IRSC charter and changes thereto

ADMR (in addition to the responsibilities of all Associate Directors)

- Serve as the Directive Owner for this order

CSO

- Serve as the Directive Owner for all suborders and suborder-specific directives under this order
- Ensure the maintenance of NIST's ionizing-radiation-safety programs

IRSC

- Oversee the effectiveness of the implementation and maintenance of NIST's ionizing-radiation-safety programs
- Recommend actions to the NIST Director as necessary on issues related to ionizing radiation safety and regulatory and license compliance
- Evaluate the adequacy of resources for NIST's ionizing-radiation-safety programs and recommend changes to the NIST Director
- Report to the NIST Director at least annually on the status of NIST's ionizing-radiation-safety programs [at intervals not to exceed fifteen (15) months]
- Review, for completeness and accuracy, Applications for License Amendment, responses to Requests for Additional Information, Licensee Event Reports, and responses to Notices of Violation, prior to their submittal to the NRC⁴
- Review for completeness and accuracy applications to transfer ownership or control of licensed activities prior to the submittal of such applications to NIST Director

⁴ Condition 8 of the Confirmatory Order issued by NRC to NIST on March 1, 2010 required NIST to incorporate language to this effect into the IRSC charter.

- For the following types of events, review the adequacy of the investigations, their conclusions, and actions to preclude their recurrence; track and report to the NIST Director on their completion:
 - NRC-reportable occurrences
 - NRC-identified violations of NIST ionizing-radiation-safety program requirements;
 - Self-identified apparent violations of NIST ionizing-radiation-safety program requirements that could be characterized by the NRC as Severity Level I, II, or III violations
 - Any incidents identified to the IRSC by the RSO that have, or may have, adverse impacts on ALARA, radiation safety, or regulatory compliance
- Review the results of internal and external audits of NIST's ionizing-radiation-safety programs; track and report to the NIST Director on the resolution of all reported findings and apparent violations
- Implement IRSC procedures necessary to meet regulatory and other program requirements

NIST Gaithersburg and Boulder RSOs

- Maintain NIST's ionizing-radiation-safety programs
- Work with the ADLP, ADMR, and the OUs as necessary to support their part of the implementation of NIST's ionizing-radiation-safety programs

NIST Gaithersburg RSO

- Maintain IRSC documents and written records of IRSC activities

Organizational Unit (OU) Directors (including the CSO)

- Ensure the implementation of NIST's ionizing-radiation-safety programs in their respective OUs
- Ensure proper allocation of resources for ionizing radiation safety in their respective OUs
- Ensure that individuals in their respective OUs are held accountable for meeting NIST's radiation-safety-program requirements
- Provide direction on significant issues involving worker safety, regulatory compliance, and environmental impacts within their respective OUs

All Individuals and Entities with Roles in NIST's Ionizing-Radiation-Safety Programs

- Carry out their program-specific responsibilities as delineated in NIST ionizing-radiation-safety programs

DELEGATIONS OF AUTHORITY

CSO

- To approve all suborders and suborder-specific directives under this order, and changes thereto

IRSC, IRSC Chair, and RSOs

- To stop immediately any operations involving the use of licensed radioactive material or ionizing-radiation-producing machines in which there are known or potential safety and health or regulatory compliance issues or that may result in exposures to ionizing radiation that are not ALARA

DIRECTIVE OWNER

13 – ADMR

APPENDICES

A. Revision History

Appendix A. Revision History

Revision	Date	Responsible Person	Description of Change
Initial	8/8/2013	Rich Kayser	Original draft
Rev. .01	8/13/2013	Dan Cipra	Formatting changes
Rev. .02	11/14/2013	Dan Cipra	Accepted OCC comments and all changes from OSHE
Rev. .03	08/19/2015	Rich Kayser	Align the responsibilities of the IRSC with the IRSC charter approved by the NIST Director on 10/10/2014

Environmental Management

NIST P 7300.00
Effective Date: 9/5/2012

PURPOSE

To articulate NIST's commitment to carrying out its mission in an environmentally responsible manner.

SCOPE

This policy applies to all activities conducted by NIST employees and associates as part of their assigned duties.

LEGAL AUTHORITY

- [Clean Air Act, as amended, 42 U.S.C. §7401 et seq.](#)
- [Clean Water Act, 33 U.S.C. §1251 et seq.](#)
- [Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. §9601 et seq.](#)
- [Emergency Preparedness and Community Right to Know Act, 42 U.S.C. §11001 et seq.](#)
- [Federal Insecticide, Fungicide and Rodenticide Act, 7 U.S.C. §136 et seq.](#)
- [National Environmental Policy Act, 42 U.S.C. §4321 et seq.](#)
- [Resource Conservation and Recovery Act, 42 U.S.C. §6901 et seq.](#)
- [Safe Drinking Water Act, as amended, 42 U.S.C. §300f et seq.](#)
- [Toxic Substances Control Act, 15 U.S.C. §2601 et seq.](#)
- [Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management \(2007\)](#)
- [Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance \(2009\)](#)
- [Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations \(1994\)](#)
- [Department of Commerce Organization Order 30-2A, National Institute of Standards and Technology](#)

POLICY

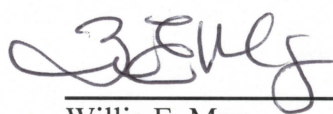
It is NIST policy to carry out all activities in a manner that minimizes environmental impacts, conserves natural resources and provides effective stewardship of the environment. To that end, NIST is committed to making environmental management an integral core value and vital part of the NIST culture by:

- Integrating environmental considerations into work practices at all levels;
- Informing employees and associates of applicable environmental regulations and NIST requirements;
- Providing the resources necessary for employees and associates to conduct their work in accordance with applicable environmental regulations and NIST requirements;
- Developing environmental goals and targets relevant to NIST operations and taking actions to achieve those goals and targets;
- Promoting pollution prevention, waste minimization, and conservation;
- Promoting the effective use of innovative environmental technologies and practices;
- Fostering a work environment in which employees and associates are encouraged to report and raise environmental issues without fear of retaliation;
- Continually improving the effectiveness and efficiency of environmental management through assessments and performance and cost metrics; and
- Complying with applicable laws, regulations and other promulgated environmental requirements.

In addition, every individual at NIST is expected to:

- Conduct their assigned duties in a manner that complies with applicable environmental regulations and NIST requirements;
- Continually strive to improve environmental performance in their work area;
- Be aware of the potential environmental consequences of their actions at all times and take care to minimize any adverse consequences;
- Promptly report or otherwise address conditions that could result in a spill or release of hazardous or regulated material to the environment;
- Promptly report environmental incidents, i.e., events in which a spill or release of hazardous or regulated material to the environment occurred or could have occurred;
- Participate in the conduct of incident investigations;
- Effectively disseminate information and lessons learned from any incidents; and
- Correct deficiencies and take actions to prevent incidents from occurring.

The Associate Director for Management Resources shall ensure the development of other directives necessary for the full and effective implementation of this policy.



Willie E. May
Director

7/24/15

Date

Environmental Management

NIST O 7301.00

Document Date: 08/28/2014

Effective Date: 11/5/2014

PURPOSE

This purpose of this Order is to define (a) the requirements of the NIST Environmental Management System (EMS) necessary for the full and effective implementation of NIST P 7300.00, Environmental Management, and (b) the roles, responsibilities and authorities of NIST management and staff for ensuring that these requirements are met.

APPLICABILITY

The NIST EMS applies to all environmental aspects of NIST operations and services and describes how these aspects are to be managed.

This Order applies to all activities conducted at the NIST Gaithersburg, Boulder, Fort Collins, and Kauai sites by (a) NIST employees, and (b) NIST associates who have signed agreements to comply with NIST and sponsoring Organizational Unit administrative requirements.

This Order supersedes Administrative Manual subchapter 12.05, Environmental Management Systems Program.

LEGAL AUTHORITIES AND REFERENCES

- [NIST Policy 7300.00, Environmental Management](#) (2012)
- 5 U.S.C. § 2105, Employees
- [Clean Air Act](#), 42 U.S.C. § 7401 et seq. (1970)
- [Clean Water Act](#), 33 U.S.C. § 1251 et seq. (1972)
- [Comprehensive Environmental Response, Compensation and Liability Act](#), 42 U.S.C. § 9601 et seq. (1980)
- [Emergency Preparedness and Community Right-to-Know Act](#), 42 U.S.C. § 11001 et seq. (1986)
- [Federal Insecticide, Fungicide, and Rodenticide Act](#), 7 U.S.C. § 136 et seq. (1996)
- [National Environmental Policy Act](#), 42 U.S.C. § 4321 et seq. (1969)
- [Resource Conservation and Recovery Act](#), 42 U.S.C. § 6901 et seq. (1976)
- [Safe Drinking Water Act](#), 42 U.S.C. § 300f et seq. (1974)

- [Toxic Substances Control Act](#), 15 U.S.C. § 2601 et seq. (1976)
- [Executive Order 13693](#), Planning for Federal Sustainability in the Next Decade (2015)
- [Department of Commerce Organization Order \(DOO\) 30-2A](#), National Institute of Standards and Technology (2008)
- Department of Commerce Administrative Order (DAO) 217-16, Energy and Environmental Department (2012)
- [Department of Commerce](#) Energy and Environmental Management Manual (2012)
- Code of Federal Regulations, [Title 40, Protection](#) of Environment
- Code of Maryland Regulations, [Title 26, Department of the Environment](#)
- Code of Colorado Regulations, [Part 1000, Department of Public Health and Environment](#)
- [ISO Standard 14001:2004\(E\), Environmental Management Systems](#) – Requirements and Guidance for Use

BACKGROUND

The NIST EMS is based on the International Organization for Standardization (ISO) Standard ISO14001:2004(E), [Environmental Management Systems – Requirements with Guidance for Use](#). The NIST EMS comprises NIST P 7300.00, this order, and the environmental programs necessary to implement this order.

DEFINITIONS

Associate – An individual conducting work at NIST who is not a NIST employee (e.g., Guest Researchers, Facility users); for a list of the types of NIST associates, see <http://inet.nist.gov/tpo/services/upload/NAIS-Types-06022014.pdf>

Deployment Tools – Tools, such as forms, instructions, IT applications, training, and user guides for facilitating the implementation of directives.

Employee – For the purposes of this Order, an employee is an officer and an individual who is defined in 5 U.S.C. § 2105.

Environmental Manager – The Chief Safety Officer, who has operational jurisdiction over the EMS.

Environmental Management Plan (EMP) – A documented plan that specifies the tasks required to accomplish a goal or objective of the EMS and that includes goals and targets, individual responsibilities, and a schedule of tasks to achieve the goals and targets.

EMP Manager – An individual who has the lead on the development and implementation of an EMP.

Environmental Management System (EMS) – A network of interrelated elements that includes responsibilities, authorities, relationships, functions, processes, procedures, practices, and resources – all implemented and maintained to achieve specific environmental goals and targets and to continually improve an organization’s environmental performance.

NIST Environmental Management Committee (NEMC) – A NIST standing committee that supports the implementation and maintenance of the EMS and provides a venue for regular internal communication regarding EMS plans and progress and for Organizational Units to provide input into the EMS.

Environmental Officer – An individual designated by the Environmental Manager to implement and maintain the EMS.

Environmental Program - An environmental program consists of a suborder, suborder-specific directives, deployment tools, and required procedures, as applicable to the program area. Environmental programs are specific to environmental focus areas such as air emissions, storm water, underground storage tanks and etc. Due to variances in state environmental regulations, separate programs have been prepared for NIST sites in Maryland and Colorado. Environmental programs are available at:

<https://safetyp.nist.gov/apps/SitePages/default.aspx>.

Environmental Program Manager – Office of Safety Health and Environment staff member designated to lead an environmental program.

Organizational Units (OUs) – Term used herein to denote any of the following: the Office of the Director, the three Associate Director organizations, the two NIST Centers, the five NIST Laboratories, the two Extramural Programs, and the six Chief Offices.

ACRONYMS

CFR – Code of Federal Regulations

EO – Executive Order

EMP – Environmental Management Plan

EMS – Environmental Management System

ISO – International Organization for Standardization

NEMC –NIST Environmental Management Committee

OSHE – Office of Safety, Health, and Environment

OU – Organizational Unit

U.S.C. – United States Code

REQUIREMENTS

NIST shall comply with the applicable requirements of Title 40 of the Code of Federal Regulations, applicable requirements of state and local environmental regulations and applicable requirements of Executive Order 13693. The NIST EMS shall be based on ISO 14001:2004(E).

RESPONSIBILITIES AND AUTHORITIES

This section delineates the responsibilities of management, staff, and organizational entities with regard to the NIST EMS. Environmental programs contain additional responsibilities.

NIST Director

- Review as necessary, continue to authorize and ensure implementation of NIST's environmental policy, established by P 7300.00
- Take ultimate responsibility for environmental management and the NIST EMS, including ensuring that:
 - Roles, responsibilities and authorities relevant to the EMS are defined, documented and communicated
 - Procedures are implemented and maintained for the ongoing identification, assessment, and management of the environmental aspects of NIST operations and services
 - Procedures are implemented and maintained for identifying and accessing all regulatory and other environmental requirements that are applicable to NIST and for ensuring that these requirements are taken into account in implementing and maintaining the EMS
 - Objectives and targets consistent with NIST's environmental policy are documented and plans for achieving them are implemented
 - Appropriate education, training, and/or experience is provided to all NIST employees and NIST associates who have signed agreements to comply with NIST and sponsoring Organizational Unit administrative requirements and who perform tasks that can have a significant impact on the environment
 - Procedures are implemented and maintained for internal EMS communications at various levels and functions, and for receiving, documenting, and responding to relevant communications from external interested parties
 - EMS elements and records are appropriately documented and controlled
 - Procedures are implemented and maintained to identify potential emergency situations and plan response actions for each situation; actual emergencies are responded to effectively by NIST and, after emergencies have occurred, plans and procedures are reviewed and tested

- Procedures are implemented and maintained to monitor and measure, on a regular basis, the key characteristics of operations that can have a significant environmental impact
- Procedures are implemented and maintained for periodically evaluating compliance with applicable regulations and other requirements
- Procedures are implemented and maintained to manage actual and potential noncompliance and for taking corrective and preventive actions
- Records are maintained as necessary to demonstrate conformity by NIST to the requirements of the EMS and the results achieved
- Internal audits of the EMS are conducted at planned intervals
- Operations associated with significant environmental aspects are planned and carried out using documented operational control procedures
- Direct the implementation and maintenance of the NIST EMS
- Serve as the NIST EMS “Champion,” which includes promoting the EMS and ensuring participation of NIST management and staff
- Ensure resources are allocated to meet EMS objectives and targets, as necessary and appropriate, including human resources, specialized skills, infrastructure, technology and financial resources
- Provide direction on significant issues affecting the implementation and maintenance of the EMS, as appropriate
- Provide direction to the Environmental Manager, as appropriate
- Approve the NEMC charter

NIST Director and Associate Directors (as a Group)

- Review the EMS annually and direct actions, as necessary, to ensure its continuing suitability, adequacy, and effectiveness

NIST Associate Directors (as Individuals)

- Assist the NIST Director in carrying out his or her responsibilities
- Ensure the implementation of the NIST EMS in their respective directorates
- Monitor, ensure, and enforce the implementation of accountability in support of environmental program and regulatory compliance
- Review the NEMC charter
- Designate OU Directors to be responsible for specific Environmental Management Plans (EMPs), based on recommendations from the NEMC

Chief Safety Officer (CSO)

- Serve as the NIST Environmental Manager
- Ensure that the EMS is implemented and maintained
- Designate and oversee the NIST Environmental Officer
- Chair the NEMC
- Review NIST's environmental management policy annually and recommend changes to the NIST Director, as needed
- Identify to the NIST Director and Associate Directors the resources required to meet EMS objectives and targets, as necessary
- Report to NIST Director and Associate Directors, as appropriate, on significant issues affecting the implementation and maintenance of the EMS
- Support the NIST Director and Associate Directors in reviewing the EMS annually and ensure that appropriate actions are taken in response to their direction
- Approve environmental suborders, suborder-specific directives, deployment tools and required OU procedures necessary to implement this order
- Delegate to subordinate line managers, and other OSHE employees the authorities necessary to carry out CSO responsibilities

Environmental Management Group Leader

- Serve as the NIST Environmental Officer
- Facilitate the implementation of the NIST EMS in accordance with NIST requirements
- Maintain one or more suborders that include requirements and procedures for:
 - Identifying and communicating significant environmental aspects to the Environmental Manager and other NIST managers and staff, as appropriate
 - Identifying existing and new environmental mandates, such as Federal and State regulations and executive orders, and updating NIST requirements, as applicable
 - Periodically evaluating NIST's compliance with all environmental mandates and other applicable legal requirements
 - Dealing with actual and potential noncompliance with environmental mandates and for taking corrective and preventive action
 - Reviewing new or revised contracts and contractual arrangements to ensure EMS conformance and regulatory compliance

- Ensuring that any NIST employees or associate performing tasks that have the potential to cause significant environmental impact(s) are competent on the basis of appropriate education, training or experience and that associated records are retained
- Ensuring that appropriate internal communication among the various levels and functions of NIST are conducted, and receiving, documenting, and responding to relevant communications from external interested parties
- Controlling EMS documents and ensuring documents are properly stored, protected, retrievable, and disposed
- Identifying and planning operational controls for the NIST operations that are associated with significant environmental aspects to ensure they are carried out under specified conditions
- Identifying potential emergency situations and potential accidents that could have an impact on the environment and developing plans for responding to them
- Ensuring that key parameters associated with NIST's significant environmental aspects are monitored and that all environmental monitoring and measurement equipment is calibrated or verified and properly maintained
- Preparing environmental management plans (EMPs) to address significant environmental aspects that have been identified for actions
- Ensuring that objectives and targets identified in the EMPs are measurable and consistent with the environmental policy
- Conducting periodic audits of the NIST EMS
- Maintain environmental programs for the following environmental topics:
 - Air Emissions
 - Hazardous Waste Accumulation and Disposal
 - Wastewater Management
 - Stormwater Management
 - Underground Storage Tank Management
 - Drinking Water Management
 - Spill Prevention and Control
 - National Environmental Policy Act
- Assist in the development of EMPs at the request of EMP managers

- Support the Environmental Manager in planning and conducting NEMC meetings and in ensuring appropriate follow-up actions
- Annually present the register of significant environmental aspects to the NEMC for review and update
- Report significant issues affecting the implementation and maintenance of the EMS to the Environmental Manager
- Facilitate annual reviews of the EMS by the NIST Director and Associate Directors
- Designate Environmental Program Managers
- Oversee the implementation of all NIST environmental programs
- Serve as NIST's point of contact for all outside agencies in regard to all environmental issues, or designate a point of contact

NIST Environmental Management Committee (NEMC)

- Annually review the register of NIST's significant environmental aspects and recommend changes, as needed
- Review EMS objectives and targets and progress in meeting those targets
- For each goal and objective of the EMS, including individual requirements from external mandates, recommend to the appropriate Associate Director an OU Director to be responsible for overseeing the development and implementation of an EMP to meet that requirement
- Review and provide feedback to EMP Managers on draft EMPs
- Review and provide feedback to EMP Managers on progress in meeting the objectives and targets of EMPs and recommend changes to the EMPs as appropriate
- Communicate EMPs and any modifications to OU Staff
- Annually review NIST's environmental management policy at the request of the Environmental Manager and recommend changes, as needed

NIST OU Directors and Subordinate Line Managers

- Ensure that their personnel are adequately instructed and informed regarding EMS goals and issues pertinent to their specific assignments
- Ensure that their organizations implement the NIST EMS, including any EMPs, as applicable to their operations
- Ensure that new or modified operations or activities are evaluated properly to identify new environmental aspects in a timely manner

- Ensure that all environmental compliance and EMS conformance issues are promptly reported to the NIST Environmental Officer, investigated, and corrected
- Communicate environmental procedures, changes in procedures, results of incident investigations, and other significant environmentally-related information to their personnel and others, as appropriate
- Assign OU employees to serve as EMP Managers or participate in the planning and implementation of an EMP relevant to the OU. Assignments related to the EMS shall be collateral duties.
- Ensure that OU employees carry out their responsibilities as defined in the EMP
- When given responsibility for a particular EMP, serve as a member of the NEMC
- Ensure that operating plans and budgets provide adequate resources for EMS activities
- Establish and communicate OU-specific environmental requirements, beyond those of the NIST EMS, deemed necessary to carry out their responsibilities under this order
- Delegate to subordinate line managers and other OU staff members, including OU/division safety personnel, the authorities necessary to carry out OU Director responsibilities

EMP Managers

- Prepare and submit draft and revised EMPs to the NEMC for review and feedback, and respond to the feedback, as appropriate
- Oversee and ensure the timely completion of tasks defined in the EMP to meet the goals and targets of the EMP
- Report to the NEMC, at the request of the Chair, on progress in meeting the goals and targets of the EMP, and respond to NEMC feedback, as appropriate

Environmental Program Managers

- Maintain environmental programs
- Submit environmental-program documentation to the NIST Environmental Officer and Manager for review and approval
- Review program documentation at a minimum every three years and revise as needed
- Oversee program implementation
- Assess compliance with program requirements and report findings to the Environmental Officer and Manager
- Document corrective actions and resolution of any findings

DIRECTIVE OWNER

150 - Chief Safety Officer

APPENDICES

A Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/29/2014	Richard Kayser(CSO)	First Draft
Rev. .01	8/29/2014	Dan Cipra	Formatting Changes Only
Rev. .02	10/28/2014	Dan Cipra	Incorporated all DRB Comments and finalized.
Rev. .03	8/21/2015	Dan Cipra	Incorporated all of OCC “Interim Review” comments.

Fire and Life Safety

NIST O 7401.00

Document Date: 01/23/2017

Approval Date: 2/3/2017

Effective Date:¹ 2/3/2017

PURPOSE

The purpose of this directive is to delineate the requirements, roles, responsibilities, and authorities necessary for the full and effective implementation of NIST Policy for Fire and Life Safety (FLS) (NIST P 7400.00).

APPLICABILITY

This order applies to NIST employees and covered associates at any NIST workplace.

LEGAL AUTHORITY AND REFERENCES

- [15 United States Code \(U.S.C\) §2227, Federal Fire Prevention and Control Act of 1974, as amended](#)
- [29 Code of Federal Regulations \(CFR\) Part 1910. Subpart L, Fire Protection](#)
- [29 CFR Part 1926, Subpart F, Fire Protection and Prevention](#)
- [Office of Personnel Management Qualification Standard for the Fire Protection Engineering Series, 0804](#)
- [NIST Policy 7400.00: Fire and Life Safety](#)
- International Building Code (IBC), 2015 edition
- International Existing Building Code (IEBC), 2015 edition
- International Fire Code (IFC), 2015 edition
- International Mechanical Code (IMC), 2015 edition

REQUIREMENTS

- NIST shall adopt codes and standards, within FLS suborders, as minimum requirements for fire and life safety on all sites owned and operated by NIST.
- The NIST Chief Safety Officer (CSO) shall designate, in writing, a NIST Authority Having Jurisdiction (AHJ), with the minimum qualification set forth below, to ensure compliance with the adopted codes and standards set forth in the FLS suborders.

¹ For revision history, see Appendix A.

- The NIST AHJ shall be a Fire Protection Engineer (FPE) who meets the minimum qualifications set forth by the [Office of Personnel Management Qualification Standard for the Fire Protection Engineering Series, 0804](#)
- The FLS suborders shall address, at minimum, the following:
 - Design and Construction of Fire Protection and Life Safety Systems in New and Existing Buildings;
 - Inspection, Testing, and Maintenance (ITM) of Fire Protection and Life Safety Systems;
 - Fire Protection and Life Safety System Impairments; and
 - Fire Prevention During Hot Works.
- NIST shall, at minimum, comply with the requirements set forth in the 2015 ICC suite of codes, including the International Building Code, the International Existing Building Code, the International Fire Code, the International Mechanical Code, and the reference standards cited within those codes, except as modified in this order and other FLS directives.
- NIST shall, at minimum, comply with the requirements set forth in the additional NFPA codes listed within Appendix B of the 2015 ICC suite of codes and those referenced within FLS suborders.
- All requests for variances, including equivalencies and exceptions, to fire and life safety codes or standards shall be submitted by a Division Chief or equivalent, or a higher-level manager, to the NIST AHJ.
 - The request for a variance (RFV) shall:
 - Be consistent with the general intent and purpose of the codes;
 - Not be detrimental to the public health, safety, and general welfare on NIST sites; and
 - Demonstrate at least one of the following, with no technical alternative existing:
 - ◇ The code and/or standard cannot be technically executed; or
 - ◇ Execution of the codes and standards will increase a hazard or create a new hazard.
 - The RFV shall include:
 - Written justification;
 - Hazard analysis;
 - Alternatives considered; and
 - Other pertinent data.

- The NIST AHJ shall provide a written response approving or disapproving the RFV².
- Approvals apply only to the specific project indicated in the RFV; prior approvals by the NIST AHJ do not constitute approval for any upcoming or future cases that are similar.
- Approvals for variances may have an expiration date depending on the nature of the request.
- All appeals of denied RFVs shall be submitted to the NIST CSO.
 - The appeal to the NIST CSO shall include:
 - ◇ The original RFV submitted to the NIST AHJ;
 - ◇ The written response from the NIST AHJ; and
 - ◇ Any other information requested by the NIST CSO.
- The NIST CSO shall provide a written response approving or disapproving the appeal, after consulting as necessary with independent subject matter experts.³

DEFINITIONS

Acting Authority Having Jurisdiction – A qualified⁴ FPE in the Office of Safety, Health, and Environment (OSHE) designated by the CSO to be temporarily assigned all authorities, duties, and obligations of the NIST AHJ during the NIST AHJ’s absence or in the event of position vacancy.

Appeal – A process by which a Division Chief or equivalent, or a higher-level manager, requests that the NIST CSO review a denial or rejection of an RFV by the NIST AHJ.

Associate – An individual conducting work at a NIST workplace who is not a NIST employee. For a list of NIST associate types, click [here](#).

Authority Having Jurisdiction – A qualified⁵ FPE in OSHE designated by the NIST CSO to enforce⁶ the NIST-adopted codes and standards relevant to fire and life safety on NIST-owned and operated sites.

Compliance – Meeting or exceeding an applicable requirement(s) of a NIST adopted code(s) and/or standard(s).

Covered Associate – A NIST associate permitted to perform work at a NIST workplace and subject to NIST policies and procedures to the extent allowed by law and the terms of the associate’s agreement. Covered associates include Foreign and Domestic Guest Researchers

² The time required for review will be determined by the complexity of the request, and the resources needed to review the request.

³ *Ibid.*

⁴ See requirements for Office of Personnel Management [Fire Protection Engineering Series 0804](#).

⁵ *Ibid.*

⁶ Nature of enforcement is dependent upon the severity of the violation, e.g. stop work, revoke permit, denial of use and occupancy, etc.

(including contractors who perform NIST R&D/technical work); Research Associates; Intergovernmental Agency Personnel Act assignees; Facility Users; Volunteer Students; and other federal employees who perform work at NIST workplaces.

Delegated Authority Having Jurisdiction – A qualified engineer in OSHE designated by the AHJ to enforce the NIST-adopted codes and standards that fall within their relevant discipline(s).

Equivalency – A proposed alternative means of providing an equal or greater degree of safety than that afforded by strict conformance to prescribed codes and standards.

Fire and Life Safety – The protection of life and property by minimizing fire and related hazards through the incorporation of and maintenance of building features, fire protection systems, and egress components, and the implementation of safe work practices.

FLS Program – A FLS suborder; all supporting suborder-specific directives, including procedures, guidance, and notices; and any associated FLS deployment tools and Organizational Unit (OU) procedures.

FLS Program Manager – For a given FLS program, an OSHE staff member assigned by the NIST CSO to manage that program.

Hot Work – Work involving welding, brazing, open flame soldering, heat treating, grinding, thawing pipes, powder driven fasteners, hot riveting, torch-applied roofing, or any other process requiring use of a spark, flame, or heat.

NIST Workplace – An establishment at one geographical location at which work-related activities are conducted by NIST employees or covered associates. NIST workplaces include sites owned and operated by NIST and by other organizations.

Organizational Unit – Term used herein to denote any of the following: Office of the Director; the immediate office of a NIST Associate Director; a NIST Laboratory; a NIST Extramural Program; or a NIST Chief Office.

Shall/Should/May –

- **Shall (Must or Will):** Indicates that the performance of an item is mandatory.
- **Should:** Indicates that the performance of an item is not mandatory, but the full implications of not performing that item must be understood and either justified or carefully weighed before choosing a different course.
- **May:** Indicates that the performance of an item is at the discretion of the individual responsible for the action.

Variance – An equivalency or an exception (i.e. modification) from the code and/or suborder requirement(s).

ACRONYMS

AHJ – Authority Having Jurisdiction

CFR – Code of Federal Regulations

CSO – Chief Safety Officer

FLS – Fire and Life Safety

FPE – Fire Protection Engineer

ICC – International Code Council

NFPA – National Fire Protection Association

NIST – National Institute of Standards and Technology

OU – Organizational Unit

RFV – Request for Variance

RESPONSIBILITIES

NIST Director

- Ensure proper allocation of resources for FLS at NIST;
- Enforce accountability for meeting NIST’s FLS program requirements;
- Provide direction as necessary on significant issues involving FLS and regulatory compliance at NIST;
- Provide direction to the NIST Associate Directors, OU Directors, CSO, and AHJ as necessary; and
- Ensure that employees and covered associates are not subject to restraint, interference, coercion, discrimination, or reprisal for reporting hazardous situations or participating in FLS program activities.

NIST Associate Directors

- Support the NIST Director in carrying out the Director’s responsibilities with respect to FLS at NIST;
- Ensure that the requirements of NIST’s FLS programs are fully implemented in their respective directorates;
- Ensure proper allocation of resources for FLS to the extent possible in their respective directorates; request additional resources as necessary;
- Enforce accountability for meeting NIST’s FLS program requirements in their respective directorates; and
- Provides direction as necessary on significant issues involving FLS and regulatory compliance in their respective directorates.

Organizational Unit (OU) Directors

- Support the NIST Associate Directors in carrying out their responsibilities with respect to FLS at NIST;
- Ensure that the requirements of NIST's FLS programs are fully implemented in their respective OUs;
- Ensure proper allocation of resources for FLS to the extent possible in their respective OUs; request additional resources as necessary; and
- Ensure that their OUs work in partnership with OSHE to develop, implement, maintain, and continually improve the NIST FLS programs.

Division Chiefs or Equivalents, or Higher-Level Managers

- Submit requests for variances and appeals.

NIST CSO (in addition to the responsibilities for other OU Directors)

- Ensure the development, deployment, maintenance, and continual improvement of the suborders, other directives, and deployment tools necessary for the full and effective implementation of NIST P 7400.00 and this order;
- Implement mechanisms to engage the other OUs in the development, deployment, maintenance, and continual improvement of NIST's FLS programs;
- Ensure that OSHE provides high-quality services to support the implementation of NIST's FLS programs by other OUs;
- Approve changes to this order;
- Approve all FLS suborders, suborder-specific directives, and any associated deployment tools and FLS-program-required OU procedures necessary to implement this order;
- Designate an OSHE FPE to serve as the NIST AHJ;
- Designate OSHE employees to serve as FLS Program Managers for NIST's FLS programs;
- Ensure that the NIST AHJ and FLS Program Managers have the authority, resources, and training necessary to carry out their responsibilities; and
- Approve or disapprove all appeals of RFVs denied by the NIST AHJ.

NIST AHJ

- Provide final interpretations of the NIST-adopted codes and standards relevant to fire and life safety on all NIST-owned sites;
- Enforce conformance to the adopted codes and standards on all NIST-owned sites;
- Enforce industry best practices when the adopted codes and standards do not address specific issues;

- Enforce the more stringent requirement(s) when the adopted codes and/or standards conflict;
- Review all proposed changes to fire and life safety systems;
- Order the correction of any deficiencies related to fire and life safety and ensure that corrective actions have been properly implemented;
- Approve or disapprove RFVs; and
- Establish industry best practices for FLS through evaluation of techniques or methodologies employed by other federal agencies or research institutes, scientific literature or treatise, or other data or fact that provides a strong basis of opinion.

FLS Program Managers

- Develop, deploy, and maintain their assigned programs;
- Carry out responsibilities specific to their assigned programs;
- Serve as the primary points of contact and subject matter experts for their assigned programs; and
- Ensure effective communications with management and staff on program-related issues.

DELEGATIONS OF AUTHORITY

OU Directors

- Delegate to subordinate line managers and other OU staff members, including OU/division safety personnel, the authorities necessary to carry out OU Director responsibilities, provided that such assignments and delegations are not inconsistent with other FLS directives.

NIST CSO

- Delegate to the Deputy CSO, subordinate line managers, and other OSHE employees the authorities necessary to carry out CSO responsibilities, provided that such delegations are not inconsistent with other FLS directives.

NIST AHJ

- Delegate to other qualified OSHE engineers (i.e., Delegated AHJ) the authority to carry out NIST AHJ responsibilities as defined within their related programs.

DIRECTIVE OWNER

CSO

APPENDICES

A. Revision History

B. Additional NFPA Reference Standards

Appendix A

Revision History

Revision No.	Approval Date	Deployment Start Date	Effective Date	Brief Description of Change; Rationale
0	2/3/2017	NA	2/3/2017	None – Initial document

Appendix B

Additional NFPA Reference Standards

- 1 Fire Code (2015)
- 3 Hydrogen Technologies Code (2015)
- 4 Integrated Fire Protection and Life Safety System Testing (2015)
- 18 Wetting Agents (2011)
- 18A Water Additives for Fire Control (2011)
- 45 Fire Protection for Laboratories Using Chemicals (2015)
- 51B Welding, Cutting, Other Hot Works (2014)
- 53 Oxygen-Enriched Atmospheres (2011)
- 54 National Fuel Gas Code (2015)
- 67 Explosion Protection for Gaseous Mixtures in Pipe Systems (2013)
- 68 Explosion Protection by Deflagration Venting (2013)
- 70B Electrical Equipment Maintenance (2013)
- 70E Electrical Safety in the Workplace (2015)
- 75 Protection of Information Technology Equipment (2013)
- 76 Telecommunications Facilities (2012)
- 77 Static Electricity (2014)
- 79 Electrical Standard for Industrial Machinery (2015)
- 80A Exterior Fire Exposures (2012)
- 87 Fluid Heaters (2015)
- 101A Alternative Approaches to Life Safety (2013)
- 115 Laser Fire Protection (2012)
- 220 Types of Building Construction (2015)
- 232 Protection of Records (2012)
- 269 Test Method for Developing Toxic Potency Data for Use in Fire Hazard Modeling (2012)
- 270 Test Method for Measurement of Smoke Obscuration Using a Conical Radiant Source in a Single Closed Chamber (2013)
- 274 Test Method to Evaluate Fire Performance Characteristics of Pipe Insulation (2013)

- 287 Test Methods for Measurement of Flammability of Materials in Cleanrooms Using a Fire Propagation Apparatus (FPA) (2012)
- 290 Fire Testing of Passive Protection Materials for Use on LP-Gas Containers (2013)
- 291 Fire Flow Testing and Marking of Hydrants (2013)
- 550 Fire Safety Concepts Tree (2012)
- 551 Evaluation of Fire Risk Assessments (2013)
- 555 Evaluating Potential for Room Flashover (2013)
- 557 Fire Loads in Structural Fire Protection Design (2012)
- 601 Security Services in Fire Loss Prevention (2015)
- 705 Field Flame Test for Textiles and Films (2013)
- 780 Installation of Lightning Protection Systems (2014)
- 790 Third-Party Field Evaluation Bodies (2014)
- 791 Unlabeled Electrical Equipment Evaluation (2014)
- 801 Facilities Handling Radioactive Materials (2014)
- 921 Guide for Fire and Explosion Investigations (2014)
- 2010 Fixed Aerosol Fire-Extinguishing Systems (2015)
- 2112 Industrial Personnel, Flame-Resistant Garments (2012)
- 2113 Industrial Personnel, Care of Flame-Resistant Garments for Protection Against Short-Duration Thermal Exposures from Fire (2015)
- 5000 Building Construction and Safety Code (2015)

Fire and Life Safety

NIST P 7400.00
Document Date: 12/30/2016
Issue Date: 2/10/2017

PURPOSE

To articulate NIST's commitment to protecting NIST employees, associates, and visitors from Fire and Life Safety (FLS) hazards.

SCOPE

This policy applies to NIST employees and covered associates at any NIST workplace.¹

LEGAL AUTHORITY AND REFERENCES

- [15 United States Code \(U.S.C\) §2227, Federal Fire Prevention and Control Act of 1974, as amended](#)
- [29 Code of Federal Regulations \(CFR\) Part 1910. Subpart L](#), Fire Protection
- [29 CFR Part 1926, Subpart F](#), Fire Protection and Prevention
- [Department of Commerce Organization Order 30-2A](#), National Institute of Standards and Technology

POLICY

It is NIST policy to protect employees, associates, and visitors at NIST workplaces from FLS hazards. Considering safety to be the control of recognized hazards to achieve an acceptable level of risk, NIST is committed to making FLS an integral core value and vital part of the NIST culture by:

- Integrating FLS considerations into work and construction practices at all levels;
- Ensuring proper allocation of resources for FLS at NIST;
- Fostering a work environment in which employees and covered associates are encouraged to report and raise FLS issues without fear of retaliation;
- Continually improving the effectiveness and efficiency of NIST's FLS processes, systems, and capabilities through assessments and other mechanisms; and

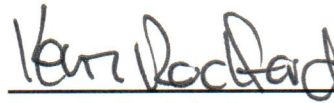
¹ For definitions of "Associate", "Covered Associate", and "NIST Workplace", see NIST O 7401.00, *Fire and Life Safety*.

- Complying with applicable laws, regulations, and other promulgated FLS requirements.

In addition, every employee and covered associate at NIST is expected to:

- Conduct their assigned duties in a manner that complies with applicable FLS regulations and NIST requirements;
- Be aware of the potential FLS consequences of their actions at all times and avoid at-risk behaviors; and
- Promptly report conditions that could result in FLS hazards.

The Associate Director for Management Resources shall ensure the development of other directives necessary for the full and effective implementation of this policy.



Kent B. Rochford
Acting Director

2/10/17

Date

Preparation and Clearance of Federal Interagency and Non-Federal Agreements

NIST O 8103.00
Effective Date: 10/13/2016

PURPOSE

This directive establishes the roles, responsibilities and requirements for execution of Federal interagency agreements and non-Federal agreements (e.g. memoranda of agreement/understanding) with other organizations under which the National Institute of Standards and Technology (NIST) will receive or provide research, goods or services. NIST E&I (expense and income) program services and goods, including but not limited to SRM (Standard Reference Materials), calibrations, NVLAP (National Voluntary Laboratory Accreditation Program) and NVCASE (National Voluntary Conformity Assessment System Evaluation) will be covered under a separate directive. Additionally, this directive establishes guidelines for enrollment in annual Federal interagency agreement and non-Federal agreement training.

APPLICABILITY

This directive is applicable to NIST employees, including administrative officers, program managers and/or principal investigators, laboratory leadership and/or scientists, and any additional NIST employees involved in the process of reviewing, approving and executing Federal interagency agreements and non-Federal agreements.

LEGAL AUTHORITIES AND REFERENCES

- [Economy Act, 31 U.S.C. § 1535](#)
- [NIST Organic Act, 15 U.S.C. §§ 271 et. seq., including but not limited to §§ 272, 273, 275a or 275b, and 278b](#)
- [Case-Zablocki Act, 1 U.S.C. § 112b](#)
- [Department of Commerce Administrative Order 218-4](#)
- [Department of Commerce Agreements Handbook](#)
- [Commerce Acquisition Manual 1317.570](#)
- [Memorandum on Case-Zablocki Act](#) Review Procedures from Cameron Kerry, General Counsel, to Secretarial Officers and Heads of Operating Units, dated May 26, 2011, delegating authority for determination of whether an agreement is an “international agreement” for agreements under \$1 million to Bureau Chief Counsel offices.

DEFINITIONS

Acceptance - *See* Fully Executed Agreement.

Accounting Classification Code Structure (ACCS) - An alphanumeric string that is used to identify and record accounting and financial information. The ACCS is also used to sort information for financial and managerial reports.

Advance of Funds - Payment by the requesting organization of the entire estimated cost of the effort at the time of agreement execution, upon the initiation of the work, or at predetermined intervals.¹

Agency Official - Highest level accepting authority or official as designated by the requesting agency and servicing agency to sign the agreement (7600A block 23). Each agency official must ensure that the general terms and conditions are properly defined, including the stated statutory authorities, and that the scope of work can be fulfilled per the agreement terms.

Assisted Acquisitions – A type of interagency agreement where the purpose of the transaction is for the serving organization to acquire goods and services by contract for the requesting agency.

Economy Act - The Economy Act of 1932, as amended, 31 U.S.C. § 1535, permits Federal Government agencies to purchase goods or services from other Federal Government agencies or other major organizational units within the same agency. An Economy Act purchase is permitted only if: (1) amounts for the purchase are actually available, (2) the purchase is in the best interest of the Government, (3) the ordered goods or services cannot be provided by contract from a commercial enterprise, *i.e.*, the private sector, as conveniently or cheaply as could be by the Government, and (4) the agency or unit to fill the order is able to provide or get by contract the ordered goods or services.

Fully Executed Agreement - Occurs *only* at the time the agreement is signed and dated by both parties. Acceptance can mean the same thing as “obligation” to requesting organizations.

Interagency Agreement (IAA) - *See* Memorandum of Understanding.

Limited Release Work - Work for other Federal agencies that may not be broadly published because the requesting organization has identified the work as For Official Use Only (FOUO), Controlled Unclassified Information (CUI), procurement sensitive information, Sensitive Security Information (SSI), Projected Critical Infrastructure Information (PCII), Sensitive But Unclassified (SBU), Dual Use Research of Concern (DURC) or other such label.

Memorandum of Understanding (MOU) - A document that describes a bilateral or multilateral agreement between parties which formalizes a working relationship. Other

¹ NIST authority for receiving advanced payment is 15 U.S.C. 275a which states “...the Secretary may require advance payment (of charges for services performed) subject to such adjustment on completion of work as may be agreed upon.” In addition, the Economy Act provides authority to accept advance payments from Federal agencies.

references to this type of agreement include: Interagency Agreements (IAA), Memorandum of Agreements (MOA), NASA Inter-Departmental Purchase Requests (NIPR), and Military Inter-Departmental Purchase Requests (MIPR).

NIST Organic Act - Also known as the “*NIST Act*”. NIST’s statutory authority to conduct most of its functions, including the authority to exercise its functions for the Government of the United States and other organizations and to accept reimbursement for the provision of such services. The NIST Organic Act includes many of NIST’s programmatic authorities and a transfer authority available only for reimbursable agreements.

NIST Resource Availability Certification for Performance of Reimbursable Work – A form included in a reimbursable agreement package, signed by the Organizational Unit (OU) Director, or if delegated by the OU Director, the OU Deputy Director, Division Chief, or technical equivalent to certify that the reimbursable agreement is NIST mission-related and that resources exist to begin the work within 120 days of agreement execution.

Non-Federal Agreement - Overarching term for all agreements that transfer funds between a non-Federal entity and NIST. They can be reimbursable or payable in nature.

Payable Agreement - Overarching term for all agreements that transfer funds from NIST to a servicing organization.

Period-of-Performance (POP) - The period of time during which work is to take place under an agreement.

Principal Investigator (PI)/ Program Manager (PM) – The person primarily responsible for the research to be performed under the agreement.²

Program Official - Division Chief, equivalent, or higher that is responsible for the work to be completed and who signs block 37 of the Treasury 7600B form.

Programmatic Authority - A Federal organization’s authority to undertake activities. For NIST, many of these authorities are contained in the NIST Organic Act.

Reimbursable Agreement (RA) - Overarching term for all agreements that transfer funds from a requesting organization to NIST.

Requesting Organization – Any non-NIST party that enters into an agreement with NIST under which NIST will provide to that party research, goods or services on a reimbursable basis.

Transfer Authority - The authority under which an agency transfers funds.³

² The PI/PMs from both NIST and the requesting organization should be listed in the agreement with their respective contact information.

³ The following transfer authorities are available to Federal organizations requesting services from NIST: Economy Act (31 USC 1535) (requires a signed *Determination & Finding Pursuant to 48 CFR, section 17.502-2* form); NIST Organic Act (15 USC 273, 15 USC 275a (or 15 USC 275b), and 15 USC 278b); Or Other Specific Agency Authorities

Treasury Forms 7600A&B - NIST's preferred template for interagency agreements.

Servicing Organization - any party that enters into an agreement to perform research, services or provide goods on a payable basis.

Statement of Work (SOW) - a formal document that captures and defines the work activities, deliverables, and timeline a servicing organization must execute in performance of specified work for a requesting organization.

REQUIREMENTS

- NIST employees shall use the Reimbursable Agreements Coordination Office (RACO) agreement process for review, approval and execution of Federal interagency and non-Federal agreements.
- NIST employees shall use [agency-specific templates](#) when applicable; for agencies without a pre-negotiated template, NIST prefers the use of the 7600A&B forms. If an alternate format is required by the sponsoring agency, contact the RACO group leader.
- NIST employees will ensure that the RA's SOW meets at least one of the [Criteria for NIST Acceptance of Reimbursable Work](#).
- NIST employees shall complete annual training courses to remain current on Federal interagency and non-Federal agreement review, approval and execution processes.⁴

RESPONSIBILITIES

Organizational Unit (OU) Director

- Certifies that the work described in the proposal/SOW tasks is properly aligned with the mission of NIST and the submitting OU, and that it can be accomplished by NIST and the submitting OU.
- Certifies that appropriate current NIST resources (staff and facilities) exist to begin this work within a reasonable timeframe, i.e. within NIST's required maximum of 120 calendar days from the date of the last signature on the agreement.
- Certifies work to be performed can be accomplished within the requesting organization's funding availability and performance period, and is in compliance with NIST legal policies.
- Certifies that, for each agreement with a Federal agency whose funds covered by the agreement expire within that 120 calendar period, work will be completed within that

⁴ Online training will be provided through the [Commerce Learning Center \(CLC\)](#) and delivered in person annually. Changes to the overarching process and/or templates may require more frequent training to ensure all employees receive current and relevant information. Enrollment in and successful completion of training is tracked through the CLC.

timeframe. *[If work cannot be completed prior to funds expiration, NIST should not accept the agreement.]*

- Determines whether the authority to sign the *NIST Resource Availability Certification for Performance of Reimbursable Work* will be delegated for a period not to exceed one year to any of the following: OU Deputy Director, Division Chiefs, or equivalent.
- Maintains documentation of any such delegation of authority within the research or service-providing organization, and reviews and reauthorizes the delegations on an annual basis, if appropriate.
- Ensures that the agreement's SOW meets at least one of the Criteria for NIST Acceptance of Reimbursable Work.
- Establishes administrative processes to ensure adherence to NIST financial policies found [here](#)

Division Chief or Equivalent

- Negotiates, reviews/submits formal proposals, and signs the agreement on behalf of their division or office, committing to the work.
- Determines NIST programmatic authority for the research/goods/services for inclusion in the agreement.

Principal Investigator (PI) /Program Manager (PM)

- Serves as the technical point of contact between NIST and the other organization.
- Informs the other organization's technical representative of the information that must be included within the agreement in order for it to meet DOC/NIST requirements.
- Advises OU management if research/goods/services can be delivered within the proposed period of performance, and is in compliance with NIST legal authorities and policies.
- Prepares description of research/goods/services in layman's terms.
- Responds to agreement questions regarding the technical aspects of the research/goods/services.

Administrative Officer

- Serves as the administrative point of contact between NIST and the other organization.
- Informs the other organization's administrative contact of the required financial information that must be included within the agreement in order for it to be reviewed and cleared.
- Reviews content of the incoming agreement and obtains missing information prior to submission to RACO.

- Ensures, to the maximum extent possible, agreement packages submitted to RACO are accurate and complete.
- Responds to questions regarding financial information, accounting data and other administrative information.
- Serves as principal contact for the agreement prior to submission to RACO and again after final legal clearance is achieved.

Reimbursable Agreements Coordination Office (RACO)

- Develops and maintains NIST-wide processes for review, approval and clearance of Federal interagency and non-Federal agreements.
- Determines needs and opportunities for improving such processes.
- Coordinates and develops agreement review process training programs.
- Maintains internal and external websites for communicating agreement requirements, information, processes, and relevant documents.
- Serves as coordinator for agreement progress, tracking, and monitoring until agreement clearance.
- Partners with internal and external stakeholders to improve agreement processes, promote efficiencies and resolves agreement issues.
- Serves as principal administrative contact from the point of submission of a complete agreement package up until the point of final legal clearance.

Office of the Chief Counsel for NIST (OCC/NIST)

- Reviews Federal and non-Federal reimbursable agreements for programmatic and legal issues including programmatic authority, and adherence to NIST policies.
- Reviews and issues final clearance for all non-Federal agreements using the NIST Working Capital Fund (WCF) non-Federal template consistent with DOC/GLD (General Law Division)'s waiver of the Department's requirement that such agreements be sent to it for review, so long as the template is not modified.
- Reviews and issues final clearance for all amendments effecting no-cost time extensions when the amendment is the first no-cost time extension for the agreement and the amendment does not extend the end date of the agreement beyond the period of availability of the other agency's funds, consistent with DOC/GLD's waiver of the Department's requirement that such amendment be sent to it for review.
- Reviews foreign agreements and coordinates with the International and Academic Affairs Office (IAAO) to obtain approval.
- Determines whether foreign agreements under \$1 million are "international agreements" under the Case-Zablocki Act.

International and Academic Affairs Office (IAAO)

- Reviews all foreign reimbursable agreements.

DOC Office of Assistant General Counsel for Administration, General Law Division (DOC/GLD)

- Reviews interagency agreements for adherence to appropriation laws and other statutes of general department or Government-wide applicability.
- Reviews non-Federal reimbursable agreements that do not follow the established non-Federal template as determined by DOC/GLD.
- Issues final clearance memoranda to RACO with a copy to NIST Finance Division.

Office of Financial Resource Management, Finance Division

- Reviews interagency and non-Federal agreements for financial information.
- Post-clearance activities listed [here](#)

DIRECTIVE OWNER

140.01 - Office of Acquisition and Agreements Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	5/12/2016	Megan Boblitt	First Draft
Rev. .01	6/30/2016	Dan Cipra	Formatting updates only.
Update	7/8/2016	Megan Boblitt	Changes Incorporated/Accepted
Update	8/17/2016	Megan Boblitt	Consolidated Payable Order with Reimbursable Order and incorporated DRB comments.
Update	9/15/2106	Megan Boblitt	Partnered with members of the DRB that did not provide concurrence and finalized the directive.

Government Purchase Card Program

NIST O 8201.00
Effective Date: 11/18/2016

PURPOSE

This directive establishes the requirements, and roles and responsibilities for the National Institute of Standards and Technology (NIST) Government Purchase Card Program in support of the Department of Commerce's (DOC) Government Purchase Card Program and in accordance with the General Service Administration's SmartPay2 Program.

BACKGROUND

Executive Order 12931 "Federal Procurement Reforms" dated October 13, 1994, sets forth requirements for Federal agencies to establish programs reducing administrative costs and other burdens that the acquisition function may impose on the Federal Government and private sector. In accordance with the Federal Acquisition Regulation (FAR) 13.201 (b), the Government-wide commercial purchase card shall be the preferred method to purchase and pay for micro-purchases.

APPLICABILITY

The NIST Government Purchase Card Program applies to all NIST Card Holders, Approving Officials, Check Writers, Funds Approving Officials and all DOC bureaus serviced by the NIST Government Purchase Card Program in accordance with their intra-agency agreements.

LEGAL AUTHORITIES AND REFERENCES

- [Executive Order 12931, Federal Procurement Reforms](#)
- [Executive Order 13423, Strengthening Federal Environmental, Energy and Transportation Management](#)
- [Government Charge Card Abuse Prevention Act of 2012 Treasury Financial Manual \(TFM\) 4-4500](#)
- [OMB Circular A-123, Appendix B](#)
- [Federal Acquisition Regulation](#)
- [DOC Commerce Acquisition Manual \(CAM\) 1313.301](#)
- [NIST Directive PR 6106.01](#)
- [NIST Government Purchase Card Handbook](#)

DEFINITIONS

- Please see Appendix A of the Commerce Acquisition Manual ([CAM](#)) for definitions.

REQUIREMENTS

- Cardholders, Approving Officials and Check Writers must be current, permanent full-time DOC employees whose current appointments have durations exceeding one (1) year as noted in CAM.
- Cardholders, Approving Officials and Check Writers must complete the training detailed in CAM, Section 2 and the NIST Purchase Card Handbook.
- Cardholders, Approving Officials and Check Writers are required to retain copies of all supporting documents pertaining to each purchase for six (6) years as detailed in CAM 3.14. The Agency Program Coordinator must ensure reconciliation files are transferred to cardholder's new Approving Official upon reassignment of Cardholder as noted in CAM 2.5. In the event both Cardholder and Approving Official depart NIST, the Agency Program Coordinator shall retain custody of the reconciliation files.
- Cardholders, Approving Officials and Check Writers shall ensure that the fully burdened price (to include shipping and any other associated fees) is authorized by the Funds Certifying Official prior to each purchase. In the event that additional funding is needed, the purchase must be authorized again prior to any additional work proceeding.
- Cardholders, Approving Officials and Check Writers shall comply with purchasing guidelines contained in CAM 3.1
- Cardholders, Approving Officials and Check Writers shall review the list of restricted items prior to making a purchase as detailed in the NIST Government Purchase Card Handbook and obtain an approved waiver prior to purchase of any restricted item in accordance with CAM 3.9 and the Purchase Card Handbook.
- Cardholders, Approving Officials and Check Writers shall consider [required sources of supply](#) in accordance with FAR Part 8 and CAM 3.4 prior to obtaining product or services from a commercial source. In addition, Cardholders, Approving Officials and Check Writers shall consider [strategic sourcing](#) requirements in accordance with CAM 3.5.
- Cardholders, Approving Officials and Check Writers shall consider small business when making micro-purchases in accordance with CAM 3.1.
- Cardholders, Approving Officials and Check Writers shall comply with Section 508 of the Rehabilitation Act of 1973 in accordance with CAM 3.8.
- Cardholders, Approving Officials and Check Writers shall purchase green products and services to the maximum extent practicable in accordance with FAR Part 23, CAM 3.7 and EO 13423.

- Cardholders and Check Writers shall obtain authorization for the “fully burdened price” from their assigned Approving Official prior to each purchase. If there are changes to the initial purchase, especially an increase in cost, approval must be obtained again.
- Cardholders, Check Writers and Approving Officials shall not use the purchase card or convenience check to pay any unauthorized commitments. Cardholders, Check Writers and Approving Officials shall refer the requestor of an unauthorized commitment to [AMD-01-15, Ratification of Unauthorized Commitment](#) procedure for possible payment.
- Cardholders and Check Writers shall seek sales tax exemption on all purchases in accordance with the NIST Purchase Card Handbook.
- Check Writers shall comply with purchasing requirements in CAM Section 4.
- Check Writers shall only use a convenience check as a method of payment as last resort, when no other method of payment is available (i.e. purchase order) and document their files to justify its use.
- Cardholders, Approving Officials and Check Writers shall document any deviations from the Government Purchase Card Program’s requirements and provide a written justification to the transaction file to explain any deviations.
- Cardholders, Approving Officials and Check Writers shall reconcile their monthly bank statements in accordance with CAM 3.14 and NIST’s monthly reconciliation schedule.
- Cardholders, Approving Officials and Check Writers shall respond to all audit requests within the time specified.
- Cardholders may not re-delegate their cards and shall comply with the card account security measure in CAM 2.9.
- Cardholders, Approving Officials and Check Writers shall be held responsible for any intentional misuse of their purchasing authority for other than official Government business in accordance with the CAM and NIST Government Purchase Card Handbook.
- Cardholders, Approving Officials and Check Writer accounts shall be suspended for improper purchases; failure to carry out responsibilities; failure to complete the required training or upon direction in accordance with CAM 2.8.

RESPONSIBILITIES

Section 1.5 of the [CAM](#) specifies the roles and responsibilities for the purchase card program. NIST does not deviate from these responsibilities.

DIRECTIVE OWNER

140.02 - Office of Acquisition and Agreements Management

APPENDICES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial Draft	8/10/2016	Megan Boblitt	First Draft
Rev. .01	8/10/2016	Dan Cipra	Formatting updates only
Rev. 02	8/15/2016	Megan Boblitt	Updated Requirements Section
Rev. 03	8/15/2016	NIST GPC APCs	Rearranged requirements section to follow GPC program transaction flow.
Rev. 04	8/24/2016	Megan Boblitt	Revised based on initial reviewers' comments.