governmentattic.org
"Rummaging in the government's attic"

Description of document:	Twenty (20) National Archives and Records Administration (NARA) Directives/Policies, 1998-2015
Requested date:	02-February-2016
Released date:	14-April-2016
Posted date:	31-October-2016
Source of document:	FOIA Officer National Archives and Records Administration 8601 Adelphi Road, Room 3110 College Park, MD 20740 Fax: (301) 837-0293 E-mail: foia@nara.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.

-- Web site design Copyright 2007 governmentattic.org --

From: "foia@nara.gov"
Date: Apr 14, 2016 11:53:17 AM
Subject: Final Disposition, Request NARA-NGC-2016-000291

8601 Adelphi Road
Room 3110
College Park, MD 20740-6001

April 14, 2016

Re: Freedom of Information Act Request: NGC16-176

This letter is in further response to your Freedom of Information Act (FOIA) request dated February 2, 2016, and received in our office February 2, 2016 via FOIA@nara.gov. As previously mentioned in the interim response we provided on March 1, 2016, your request has been assigned the above internal tracking number, as well as the FOIAonline tracking number NARA-NGC-2016-000291. Please use both numbers when corresponding further with regard to this request. In your request, you stated: Pursuant to the provisions of the Freedom of Information Act, I hereby request an electronic/digital copy of each of the following NARA Directives/Policies:

607	Content Rules and Requirement for NARA Public Websites
817	Posting Digital Copies of High-Demand Archival Materials on NARA Websites
1202	Office of Inspector General - Investigations
1310	Review of Agency Records Storage Facilities
1310	rev 1 Review of Agency Records Storage Facilities
1403	Maintenance, Disposition and Access to records of Defunct Agencies
1441	Appraisal Policy of the National Archives and Records Administration
1462	rev 01 Replevin of Archival Materials
1463	Unauthorized Destruction or Removal of Federal Records at Agencies
1454	Destruction of Federal Records in the Custody of NARA Records Centers
1465	Physical Transfer of Perm/Temp Fed Records to NARA Rec Centers for Storage and Other Service
1501	Custody of Federal Records of Archival Value
1502	Procedures for Processing Proposals for Affiliated Archives
1561	Records Emergency Preparedness and Recovery in NARA Facilities
1601	Screening for Restricted Information in Federal Records
1602	Access to Records Requested Under the Freedom of Information Act
1701	Loans of Holdings in NARA’s Physical and Legal Custody
Files 203	NARA Files Maintenance and Records Disposition Manual
1100-02	Federal Agency Employee Contacts with Presidential Campaigns
1600-02	Investigations of Terrorist Activity

1600-03	Access to Archival Materials in the Context of Concern about Terrorism
1603-01	Initial Privacy Reviews and Privacy Impact Assessments
1603-03	Rules of Behavior Relating to the PII
1605-2	Special Access by Government Officials to Classified, Unclassified, Closed Records
1605-5	Handling of Publicly Available Records Withdrawn for Classification Purposes
1611-01	Overdue, Damaged and Missing Loans of Holdings in NARA's Physical and Legal Custody
1653-01	NARA Fees for Reproductions of Archival Official Military Personnel Files
98-205	Policy on Funding Programs and Staff in Presidential Libraries
98-234	Official NARA Representation
202-supp	Classified Information Security Program Handbook (supplement to NARA 202)
1464-supp	Disposal Procedures for Temporary Records
1571-supp	Architectural and Design Standards for Presidential Libraries
1100-01	Federal Agency Contacts with Bush-Cheney '04
1605-1	Response to Withdrawal of Declassified Records from Open Shelves
93-130	Identification of Costs — JFK Assassination Materials
99-067	Quarterly Reports to the Archivist

In response to your request, we have identified and reviewed the following 19 active NARA directives and interim guidances totaling 395 pages. Of this total, six (6) pages are withheld in part pursuant to 5 U.S.C. § 522(b)(7)(E). We are releasing the remaining 389 pages in full.

NARA 190	Office of the Inspector General – Investigations
NARA 202	supp Classified Information Security Program Handbook
NARA 807	Content Rules and Requirements for NARA Public Web Sites
NARA 817	Posting Digital Copies of High-Demand Archival Materials on NARA Web Sites
Interim Guidance 98-205	Policy on Funding Programs and Staff in Presidential Libraries
NARA 1104	Participation on Standards Bodies
NARA 1310	Review of Agency Records Storage Facilities
NARA 1403	Maintenance, Disposition and Access to Records of Defunct Agencies
NARA 1441	Appraisal Policy of the National Archives and Records Administration
NARA 1462	Recovery of Alienated Archival Materials
NARA 1463	Unauthorized Destruction or Removal of Federal Records at Agencies
NARA 1464	Destruction of Federal Records in the Custody of NARA Records Centers

NARA 1465	Physical Transfer of Permanent and Temporary Federal Records to NARA Records Centers for Storage and Other Service
NARA 1464-S1	Disposal Procedures for Temporary Records
NARA 1501	Custody of Federal Records of Archival Value
NARA 1502	Procedures for Processing Proposals for Affiliated Archives
NARA 1603	Access to Records under the Privacy Act
NARA 1611	Loans of Archival Holding to Federal Originators
NARA 1653	NARA Records Reproduction Fee Schedule

As a noncommercial FOIA requester you are entitled to receive 100 free pages. We are also providing you with an additional 98 pages free of charge for several NARA directives and interim guidances that have either been updated or were scheduled to be made publicly available online. For the remaining 197 pages the cost is $0.30 per page, which brings your total to $59.10. Please mail your payment to the National Archives at the address below; NARA accepts checks or money orders made out to the National Archives:

Trust Fund: Office of General Counsel
FOIA and Privacy Act Officer
National Archives and Records Administration
8601 Adelphi Road, Room 3110
College Park, MD 20740

This completes the processing of your request. If you are not satisfied with our action on this request, you have the right to file an administrative appeal in writing via regular U.S. mail or email. Please address it to the Deputy Archivist of the United States (ND), National Archives and Records Administration, 8601 Adelphi Road, College Park, Maryland 20740. Both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” You may also submit your appeal to FOIA@nara.gov, also addressed to the Deputy Archivist. If you submitted your initial request through FOIAonline, you may file your appeal through that web portal. Please follow the instructions provided on the FOIAonline website to appeal any decisions. Your appeal should be received within sixty (60) calendar days from the date of this letter and it should explain why you believe this response does not meet the requirements of the Freedom of Information Act. All correspondence should reference your internal case tracking number, NGC16-176, as well as FOIAonline tracking number NARA-NGC-2016-000291.

Sincerely,
Steven D. Booth
Archivist
Office of General Counsel
National Archives and Records Administration
FOIA Hotline: (301) 837-3642
Email: FOIA@nara.gov

Given the nature of this request, some records are only being released to you as the requester. If you have an account in FOIAonline, you may access those records by logging into FOIAonline. Otherwise, those responsive records will be sent via the method agreed upon with the FOIA processor.

National Archives at College Park

8601 Adelphi Road
College Park, Maryland 20740-6001

Date : August 5, 1998

Reply to
Attn of : NARA 98- 205 INTERIM GUIDANCE

Subject : Policy on funding programs and staff in Presidential Libraries

To : Office Heads, Staff Directors, ISOO, NHPRC, OIG

The policy paper attached defines the appropriate funding source for programs and positions in Presidential libraries. The paper lists many programs that fall outside of NARA's statutory responsibility or ability to fund. With funding from a library support organization, the library can legitimately expand its program into these and other related areas.

All new positions in Presidential libraries will be funded by direct funds or trust funds in accordance with the guidelines established in the policy paper. Current positions not funded in accordance with these guidelines will over time be reassigned to the appropriate funding source.

If you have any questions concerning this policy, please contact David F. Peterson by e-mail or on 301-713-6050.

JOHN W. CARLIN
Archivist of the United States

Attachment

EXPIRATION DATE: 08/05/99

Presidential Libraries and Their Support Organizations

Funding Roles

At America's Presidential Libraries, breaking with tradition *is* a tradition. Long before the term became fashionable, the Libraries incubated the concept of public--private partnerships. Built with private funds by a Foundation, institute or other support organization, the Presidential libraries are staffed, managed and maintained by the federal government. Moreover, there is nothing static about these relationships. Over time the role of Library Foundations has evolved to meet changing needs. In the process, they have contributed to the rich diversity of a system in which each Library pursues a programming agenda as distinctive as the President it commemorates. Exhibits, conferences and lectures funded by library foundations are among the special events that define a library and enlarge its role beyond a repository.

Some of these organizations have chosen to fund ambitious museum programs, over and above what is provided for by federal statute. Others have generously aided academic research, public education efforts, and a wide range of programs designed to raise the institutional profile and combat historical illiteracy. Equal only to the flexibility displayed by each Foundation is its generosity. Both qualities are essential if Presidential Libraries are to remain dynamic centers of public scholarship and service.

NARA's Funding Responsibility

Through its OE (Operating Expense budget) the federal government is responsible for funding activities mandated by law as part of NARA's mission. These include the appraisal, accessioning, processing, and preserving of materials held in the libraries, as well as the promotion of their usage by researchers. NARA must also provide for security, facility maintenance[1], and environmental and safety controls[2]. It pays salaries of administrators,

---

[1]The 1986 amendments to the Presidential Libraries Act require an endowmenet to partially offset facility maintenance costs. The Bush Library is the first library to provide for an endowment.

[2]See Appendix A for a list of NARA authorities delegated to the libraries.

archivists, archives specialists, curators, registrars, librarians, archival and museum technicians, and education specialists[3]. The agency likewise regards all facility managers, secretaries and clerks (at least those whose duties are not Trust Fund related) as OE supported positions. This list is neither exhaustive, nor conclusive. As the libraries' needs change or new jobs are created, NARA will need to reevaluate or determine the appropriate funding source.

Needless to say, this does not exhaust our institutional mission. Quite apart from legislative mandates, NARA and the Libraries acknowledge a responsibility to increase public awareness and use of materials representing the American experience in all its variety. Indeed, it is no exaggeration to say that the timely availability of such "essential evidence", most of it generated by government, poses a critical test of our democracy.

Inevitably, an activist NARA has defined more opportunities for service than sources of federal funding. As custodians of the national heritage we thus confront a painful paradox: never before have so many Americans stood to benefit so greatly from what we have to offer - and never have identifiable needs so outstripped available resources.

Assistance from Library Support Organizations

In this era of increasing demands, expanding requirements, and constrained federal budgets NARA is more reliant than ever on library support organizations for help in realizing our shared goals. There are many areas outside NARA's statutory responsibility and funding ability in which foundation support can legitimately expand a library's program. The following examples come readily to mind:

- the creation or replacement of permanent exhibits;
- the mounting of temporary exhibits that cannot be funded out of the Trust Fund
- adding or sustaining oral history programs through the provision of travel funds and/or staff;

---

[3]Only one position which represents the basic educational component would be funded out of OE. Additional education support positions should be funded out of the Library's Trust Fund.

- providing for travel to solicit new collections;
- supporting development and maintenance of a docent program;
- publishing specialized finding aids or educational materials;
- providing research grants, awards, and/or visiting scholars' programs;
- enlarging the library's book collections;
- sponsoring conferences, symposia, lectures, and video/film productions;
- underwriting paid promotion, receptions, and other public relations activities.

Trust Fund Support of Library Positions and Programs

Each Library's Trust Fund derives revenue from admissions, building use, museum shop sales, and/or reproductions of historical materials for researchers. The Trust Fund is used in turn to generate temporary exhibits, publications, library events, and income producing operations. Positions supported by the Trust Fund should be related to these functions. Salaries represent by far the largest single ongoing expense to the Trust Fund. While funding sources for library positions have been inconsistent in the past, NARA expects to correct these inconsistencies over a period of time. This means eventually moving some positions from the Trust Fund to direct and in other cases from direct to the Trust Fund.

In the meantime, this rule of thumb should prevail: all Trust Fund positions (including those supported by grants to the Trust Fund) should be income producing positions or positions that develop programs funded in whole part in part by the Trust Fund and/or grants from foundations.

Consistent with this formula, Libraries should in the future expect to support out of their Trust Funds admission and sales positions (including sales managers), other visitor services positions, tour guides, exhibit specialists, audiovisual support for exhibits and public programs, and reproduction support positions.

Strengthening the Public-Private Partnership

The Presidential Library system has never been static. Throughout its history, it has been called

upon to respond to new needs and demands, as Congress has enacted new statutory requirements for funding and records responsibility. Existing buildings become cramped and obsolete, even as limited resources must be stretched to meet the special requirements of new libraries. Accepting this reality, many Foundations have sought to redress the balance by providing additional funds with which to expand library programs, outreach, and educational enrichment. (By attracting new visitors, they have simultaneously strengthened Library Trust Funds). NARA deeply appreciates Foundation efforts to build endowments and thereby enable Libraries to offer diverse and creative programming.

Clearly, the relationship between the Libraries and their Foundations is one of mutual support and sustenance. No Library can be completely self-sustaining if admission prices are to remain affordable. Recognizing this, it falls to the Foundation to provide the critical margin of resources spelling the difference between a repository for historical documents and lively, heavily patronized classrooms of American democracy.

Working together, NARA and the various Library support organizations can sustain and extend a Presidential Library system that has served this country spectacularly well for nearly six decades. Through our partnerships we can renew for succeeding generations the eloquent assertion made by Franklin Roosevelt in dedicating his Library in 1941:

> "To bring together the records of the past and to house them in buildings where they will be preserved for the use of men and women in the future, a Nation must believe in three things.
>
> It must believe in the past.
>
> It must believe in the future.
>
> It must, above all, believe in the capacity of its own people so to learn from the past that they can gain judgement in creating their own future."

With the indispensable help of and input from their Foundations, America's Presidential Libraries will continue to supply the information and inspiration required by a free, inquisitive, and self-examining citizenry.

Appendix A: Funding Sources for NARA Authorities[4]

NARA Authorities	NARA OE	Trust Fund	Foundations
Appraise Presidential and Federal records and recommend appropriate disposition	X		
Solicit, negotiate, and review offers to donate historical materials	X		Fund travel for soliciting personal historical materials for donation to the library.
Accept for deposit historical materials determined by the Archivist to warrant continued preservation.	X		
Dispose of records and other historical materials in accordance with applicable law and regulation.	X		
Review Presidential records, Federal records, and donated historical materials for national security, statutory, and when applicable, donor's deed of gift restrictions on access.	X		
Service records and other historical materials by furnishing the records, or information from them, or copies of them, to US government agencies and the public.	X	Staff support, equipment, supplies and contracts for reproduction for fee services	Subsidies for researcher copying or reproduction support for visiting scholars' programs.
Operate research rooms for public or US government agency use of records and other historical materials or copies thereof.	X		Provide grants or funding for visiting scholars
Review and respond to FOIA requests, mandatory review requests and appeals, and appeals for access to records and other historical materials restricted by donor's deeds of gift.	X		

[4]The authorities listed here can be found in the NARA Organization and Delegation of Authority Manual (ORG/AUTH 101)

NARA Authorities	NARA OE	Trust Fund	Foundations
Establish physical and management control over the storage, arrangement, and security of records and other historical materials and the space housing them.	X		
Inspect records and other historical materials to determine the state of their preservation; identify those requiring preservation and repair or reproduction; determine the appropriate treatment; and carry out appropriate measures....	X		May at their discretion provide funding for special preservation projects such as cleaning and repairing the First Lady's dresses.
Analyze records and other historical materials...; prepare descriptive guides, lists, inventories, and other finding aids; and perform research in the administrative history of Presidential administrations.	X (NARA provides overall direction for published finding aid program)	May provide editorial support and funding for fee publications.	May at their discretion provide funding for publication of finding aids and other research materials.
Plan and conduct programs for the documentary publication of records and other historical materials.	Overall direction provided by NARA/Director	Publication for sale of documentary materials.	Publication for sale of documentary materials.
Plan and conduct oral history projects relating to the holdings of the library.	Overall direction provided by NARA/ Director		Fund oral historian, oral history travel and transcription
Exhibit records and other historical materials and assist other elements of NARA in preparation of exhibits by recommending and providing records and other historical materials from the holdings.	Overall direction and curatorial support provided by NARA/OE	Fund cost of temporary exhibits, admission staff, exhibit specialists and audiovisual support staff.	Fund permanent and temporary exhibit. Can provide admission staff in accordance with NGC memo.
Developes, provides, and promotes public and educational programs that provide for greater understanding and use of NARA's cultural services and educational resources and services by educational and research institutions and the general public.	Overall direction provided by NARA/Director	Provide staff and funds	Provide funds
Recruit and train volunteers for in-service and outreach programs.		Provide staff for coordinating program	Provide funds for recruitment and recognition of volunteers

NARA Authorities	NARA OE	Trust Fund	Foundations
Operate a museum shop, and sell publications and historical mementos.	NARA provides guidance and/or regulations	Staff and manage museum shop.	Staff and manage museum shop at library site in accordance with NGC memo.
Manage expenditures from the Library's National Archives Trust Fund Account.	X		
Administer the facilities management program of the library in coordination with NL.	X		

National Archives and Records Administration

Transmittal Memo

DATE: July 25, 2013

TO: Executives, Staff Directors, NHPRC, and OIG

SUBJECT: NARA 190, Office of the Inspector General - Investigations

Purpose: This policy clarifies employee responsibilities and OIG reporting for IG investigations.

Canceled policy or policies: This directive cancels NARA 1202, Office of Inspector General – Investigations, dated May 13, 2004.

Effective date: This policy is effective on date of signature.

Contact information: For more information on this policy, please contact John Simms, OIG, by telephone at (301) 837-1966 or by e-mail at john.simms@nara.gov.

DAVID S. FERRIERO
Archivist of the United States

National Archives and Records Administration

NARA 190
July 25, 2013

SUBJECT: Office of the Inspector General - Investigations

190.1 Purpose

This directive establishes policies and procedures for investigations conducted by the Office of Inspector General (OIG). Investigations include suspected violations of Federal laws, rules, regulations, or other administrative requirements involving NARA's programs and operations (see para. 190.5).

190.2 Authorities

a. The Inspector General Act of 1978, as amended (5 U.S.C., Appendix);

b. The Inspector General Reform Act of 2008 (P.L. 110-409);

c. The Whistleblower Protection Act of 1989 (5 U.S.C. §§ 1211 to 1219, 1221, 1222, 3352);

d. The Whistleblower Protection Enhancement Act of 2012 (P.L. 112-199);

e. Government Organization and Employees, Rights and Duties of Agencies and Labor Organizations, Representation Rights and Duties (5 U.S.C. § 7114); and

f. Government Organization and Employees, Administrative Procedure, Ancillary Matters (5 U.S.C. § 555(b)).

190.3 Responsibilities

a. **Executive/Office Head/Staff Director –**

(1) Ensure NARA employees fully cooperate with the OIG and establish a culture where employees are encouraged to freely communicate with the OIG.

(2) Respond in writing to the OIG within 45 days after receipt of a Report of Investigation requiring a response, describe what action has been taken or is planned to be taken.

b. **Inspector General (IG) –**

(1) Receive complaints and allegations connected to NARA from anyone with sufficient relevant information;

(2) Investigate complaints, at the discretion of the Inspector General or Assistant Inspector General for Investigations, and as facts and circumstances warrant;

(3) Issue reports of investigation, or other written products that may include recommendations, to the Archivist, executive, office head, staff director, or other appropriate party;

(4) Keep a record of complaints and responsive actions;

(5) Conduct proactive reviews of agency programs and operations to protect against fraud, waste, and abuse; and

(6) Report violations of Federal criminal law to the Attorney General of the United States.

c. **Assistant Inspector General for Investigations (AIGI) –** Manages the OIG Office of Investigations (OI) and liaises with Federal, state, and local law enforcement, investigative agencies, and related governmental and non-governmental entities.

d. **Employee –** Employees must report suspected criminal acts, fraud, waste, abuse, and gross mismanagement to the OIG.

(1) NARA employees shall cooperate fully with any OIG investigation; shall not withhold information or documentary materials from the OIG; shall furnish sworn oral or subscribed statements upon request, subject to subpara. d(2) of this Section; and shall answer questions relating to their employment and to matters coming to their attention in their official capacity or by reason of their employment. In conducting its investigative function, the Inspector General is authorized, under the Inspector General Act, to have access to all records, reports, audits, reviews, documents, papers, recommendations and other material available to NARA that relate to NARA programs and operations.

(2) NARA employees may assert their Fifth Amendment right to refuse to answer questions on the grounds that the answers may be used against them in a criminal proceeding. An employee who asserts his or her Fifth Amendment right against self-incrimination may not be disciplined solely for remaining silent. However, an employee's silence may be considered, in taking disciplinary action, for its evidentiary value as warranted by the facts surrounding the case.

(3) NARA employees who fail to cooperate with an OIG investigation by refusing to answer questions or otherwise cooperate may be disciplined. In the case of a criminal investigation, an employee may be disciplined for refusing to cooperate with the OIG if, after receiving either a grant of immunity from criminal prosecution or being advised of a declination of

prosecution by the Department of Justice or other prosecuting authority, the employee continues to refuse to cooperate with the investigation.

(4) NARA employees should have no expectation of privacy in NARA-provided offices or workspaces. NARA and OIG officials may search any NARA workspace at any time, for any reason. Keys and locks provided to employees for their workspaces are for the benefit and security of NARA and NARA information; they do not provide employees with an expectation of privacy and all spaces are therefore subject to search.

190.4 Reports prepared by the OIG Office of Investigations (OI)

a. Referral Memorandum - prepared when a preliminary investigation or investigative initiative results in information the OIG believes should be referred to NARA. The memorandum may be for information only or a response may be required.

b. Report of Investigation - report of alleged misconduct prepared for referral to office heads, staff directors, or senior management; or report referred to the Attorney General or law enforcement authorities for criminal or civil proceedings. When referred to NARA, the report may be for information only or a response may be required.

c. Other reports may be prepared at the discretion of the OIG when warranted by the situation. For example, the OI may prepare a Management Letter when an administrative issue is uncovered during OI work that calls for timely notification to management.

190.5 Complaints and allegations

a. OIG assessment of complaints and allegations - The OIG accepts and assesses complaints, allegations, and information concerning, but not limited to:

(1) violations of laws, rules, or regulations;

(2) instances of gross mismanagement;

(3) waste of funds; and

(4) abuse of authority.

b. Allegations received by the OIG are evaluated and, if found to have merit, pursued at the discretion of the IG or AIGI.

c. To contact the OIG, allegations and complaints can be made in person or by other methods such as by:

(1) Calling the OIG Hotline:
301-837-3500 (Washington, DC metro area)

800-786-2551 (toll-free and outside the Washington, DC metro area)

(2) Sending a fax to 301.837.3197

(3) Sending an e-mail to OIG.Hotline@nara.gov

(4) Sending a document to:
OIG Hotline
NARA
P.O. Box 1821
Hyattesville, MD 20788-0821

Online reporting and up-to-date information can be found on the OIG website.

d. Anonymous complaints and allegations are accepted, however, anonymous allegations often present the OIG with insufficient information and no ability to contact the complainant for clarification or additional information.

e. Any employee who makes a complaint, allegation, or otherwise provides information that is knowingly false is subject to disciplinary action. (See PERSONNEL 300, ch. 752, Disciplinary and Adverse Actions.)

f. For personnel-related matters (complaints and allegations), such as grievable actions and Equal Employment Opportunity complaints, contact the Office of Human Capital (H) or Equal Employment Opportunity Program Office (NEEO), as appropriate. Employees may ask the OIG for assistance if they feel that appropriate action is not taken. Contacting the OIG does not affect existing procedures for resolving employee grievances, EEO complaints, Merit System Protection Board personnel matters, or other personnel concerns.

190.6 Employee protections

Pursuant to Federal statute, the OIG can provide confidentiality to employees. The OIG generally will not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee. The OIG may disclose the identity of employees providing complaints or information if it is determined that disclosure is unavoidable. The following protections are afforded to employees:

a. Whistleblower Protection Act of 1989 and the Whistleblower Protection Enhancement Act of 2012. These laws specifically ban reprisal through personnel actions against those who allege violations. Such disclosures to the OIG are protected under this act. Further whistleblower protections may be provided under other sources, such as Presidential Policy Directive 19's prohibition on the revocation of security clearances for whistleblowing activity.

b. It is NARA policy that:

(1) Those cooperating with the OIG will not be threatened, intimidated, or subjected to reprisals. If you feel you have been treated in such a manner, or are aware of someone who may have been subjected to such treatment, contact the OIG immediately.

(2) Promises of special consideration, favors, or gifts in exchange for an individual's refusal to cooperate with the OIG are illegal. Immediately report such activity to the OIG.

(3) Employees are not required to report their contacts with the OIG to their supervisors.

190.7 Employee rights

a. Fifth Amendment protection - NARA employees may assert their Fifth Amendment right to refuse to answer questions on the grounds that the answers may be used against them in a criminal proceeding.

b. Representation rights

(1) Under 5 U.S.C. 7114, an employee in a unit represented by an exclusive labor organization has the right to request the presence of a union representative at an investigative interview when the employee believes that the review may result in disciplinary action.

(2) While the majority of OIG interviews are done on a voluntary basis, if an interview is compelled, an employee may request to have an attorney present under 5 U.S.C. 555(b).

190.8 Confidentiality of investigations

a. The OIG may request, particularly on sensitive investigations, that an employee be discrete and not disclose to any unauthorized person information provided to or received from the OIG.

b. Preserving the confidentiality of investigations is necessary to protect the privacy rights of the parties and to prevent interference with investigations (which may in some instances be construed as obstruction of justice).

c. Any official or employee who has knowledge of an OIG investigation must not, without prior written approval from the OIG:

(1) engage in any independent inquiry or investigation relating to the matter; or

(2) disclose to unauthorized persons information that identifies or could lead to the investigation of an individual who has reported the alleged violation.

d. The restrictions listed above do not prevent officials or employees from communicating with an accused or the accused's counsel in criminal proceedings.

190.9 Suspension/reassignment during an investigation

During an investigation, management may take action to relieve from duty any employee whose continued presence would constitute a danger to persons, property, and/or the performance of Government functions. This would only occur following consultation with the OIG and in accordance with suspension procedures in PERSONNEL 300, ch. 752.

190.10 Inquiries concerning NARA investigations

All inquiries regarding a pending or ongoing OIG investigation should be referred to the OIG. This includes matters under consideration by other law enforcement agencies.

190.11 Access to investigative reports

All requests for investigative reports and other documents must be referred to the OIG. The OIG will determine release of documents pursuant to the Freedom of Information Act, Privacy Act, and other related requirements.

190.12 Action by management

Within 45 calendar days after receipt of a Report of Investigation or other written referral, the deciding or responsible official (i.e., executive/office head/staff director or designee) must respond in writing to the OIG, detailing any action taken or planned in response to the report. The OIG will include the written response of action taken or planned in the OIG investigative case file.

190.13 Maintaining records created by this directive under the NARA Records Schedule

a. OIG investigative case files – Use File no. 1208-1 or -2 as appropriate for the particular investigative action.

b. Other offices' records related to specific OIG investigations – Federal Records Centers and Regional Archives should use File No. 266. Cut off records upon closeout of an investigation instead of annually as stated in the 266 disposition instructions. All other NARA units should use File no. 110, Routine Program Administration Files. Cut off records upon closeout of an investigation instead of annually as stated in the 110 disposition instructions.

National Archives and Records Administration

CLASSIFIED INFORMATION SECURITY PROGRAM HANDBOOK

Supplement to NARA 202

February 23, 2015

TABLE OF CONTENTS

Section & Title **Page**

Section & Title **Page**

CHAPTER 3 – ACCESS

CHAPTER 4 – SAFEGUARDING

Section & Title **Page**

CHAPTER 5 – TRANSMISSION

Section & Title **Page**

CHAPTER 6 – DECLASSIFICATION AND RECLASSIFICATION

CHAPTER 7 – DISPOSAL AND DESTRUCTION

CHAPTER 8 – SECURITY EDUCATION, TRAINING, AND AWARENESS

Section & Title **Page**

Chapter 1

OVERVIEW

1.1 Introduction

This handbook defines classified national security information and provides the detailed procedures for managing and safeguarding it within the National Archives and Records Administration (NARA). It implements NARA 202, Classified Information Security Program, and pertains to all NARA records, regardless of media, including operational records, accessioned records, donated historical materials, any records transferred to NARA archival facilities or records centers in the legal or physical custody of NARA, and information generated by NARA.

The intent of this handbook is to serve as a "how to" guide that the NARA Information Security Officer (ISO) and Information Security Program Managers (ISPMs) use to promote a viable and dynamic classified information security program at all locations within the agency. It further serves as a resource for every NARA employee with access to classified national security information to understand and faithfully discharge their responsibilities for protecting the information with which the Nation has entrusted them. In fact, this handbook is a valuable tool that every employee and contractor who works at a NARA facility must follow to protect all forms of classified information and help the agency maintain a sound overall security profile.

All general references to NARA 202 in this handbook signify both the directive and the handbook.

Classified National Security Information (hereafter in this handbook also referred to as *"classified information"*) is information that has been determined pursuant to Executive Order (E.O.) 13526, Classified National Security Information, or any predecessor Executive orders to require protection against unauthorized disclosure in the interest of national security and is marked to indicate its classified status when in documentary form. Classified information falls into one of three basic classification levels: Top Secret, Secret, or Confidential. The designation Unclassified is used to identify information that does not require a security classification.

1.2 Policy

The Executive for Business Support Services (B) has been appointed by the Archivist to act as the Senior Agency Official (SAO) under section 5.4 of E.O. 13526, to direct and oversee NARA's classified information security program. The NARA Information Security Officer (ISO) is charged by the SAO to administer and manage the program, complying with all appropriate governing authorities in implementation of the following overall policy:

a. classified information must be identified, controlled, safeguarded, and declassified in accordance with this handbook;

b. declassification of information receives emphasis due to NARA's important role in ensuring that information remains classified only as long as required in the interest of national security; and

c. management of classified information is included as a critical element or item to be evaluated in the rating of original classification authorities; security managers or specialists; and all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

1.3 Information Technology (IT) Systems Guidance

All NARA IT systems processing or storing classified information must be designed and operated in a manner to protect the availability, integrity, and confidentiality of the information.

a. NARA 202 provides the necessary guidance for the protection of classified information before it is entered into an IT system, classified output that has been generated from the system, and for the physical environment surrounding the system.

b. NARA 804, Information Technology (IT) Systems Security, establishes NARA policies, roles and responsibilities for securing all IT systems used or operated by, or on behalf of NARA, and the information that is collected or maintained within those systems.

1.4 Other Guidance References and Electronic Links

This handbook contains references and some links to cross-referenced areas within the handbook and to other relative policy issuances. If readers find a reference that they believe is not valid or current, or a non-working link, please contact the Information Security Officer for correction.

Chapter 2

[Return to TOC]

IDENTIFYING MARKINGS

2.1 General

NARA does not have original classification authority. This chapter primarily discusses identification and markings for the purpose of working with classified information contained in the records of other agencies that do have original classification authority. NARA does, however, have the authority to classify information derivatively in accordance with E.O. 13526, as amended, and as explained in par. 2.2 of this handbook.

a. All classified information must be clearly identified and designated by appropriate markings. Markings used to identify classified information are limited to the terms Top Secret, Secret, and Confidential. These terms must not be used on unclassified executive branch information, such as Personally Identifiable Information (PII). Caveats or warnings may be added to control or restrict access for special categories of classified information as described in par. 2.10. The term "markings" includes both electronic and physical labeling or other identification of material. Markings are the principal means to recognize and convey the necessary protection requirements for classified information. Markings:

(1) alert holders to the presence of classified information;

(2) identify, as specifically as possible, the exact information needing protection;

(3) indicate the level of classification assigned to the information;

(4) provide guidance on downgrading and declassification;

(5) give information on the source(s) of and reasons for classification of the information; and

(6) warn holders of any special access, control, or safeguarding requirements.

b. The Information Security Oversight Office (ISOO) booklet, “Marking Classified National Security Information,” describes in detail the essential markings required under E.O. 13526, and is a handy reference guide to use in identifying and protecting classified information. Contact your ISPM for further information.

c. Markings are hand-stamped, printed, or affixed (with a sticker, tape, etc.).

d. Historical Records:

(1) NARA has also received and holds millions of historical documents that were marked under previous executive orders or contain no markings. Par.

2.8 of this chapter also discusses some older markings that will be found in historical materials and describes some types of materials that may contain unmarked classified information. Classified information in unmarked documents is initially identified based on content and reviewer expertise and subsequently confirmed by the equity holder.

(2) Some historical documents may not be marked at the top and bottom of the page, but only have portion markings (classification marking for a paragraph or part of a document that pertains only to that specific section of the document) with either (C) (S) or (TS) identifying the classification level of a particular paragraph. Documents may only be marked as classified on the cover page or the beginning page, which requires the entire document to be protected as classified absent any other indication to the contrary, e.g., subsequent page or paragraphs marked at a different classification level or as unclassified.

e. Application of markings at NARA should be limited to operational files, including those derived from originally classified documents, or in accordance with instructions from the original classifier or applicable security classification guides.

2.2 Derivative Markings

Derivative classification is incorporating, paraphrasing, restating, or generating already classified information in new form and marking it consistently with the same information or guidance contained in the source document. Additionally, the compilation of unclassified information may reveal a new aspect of information that meets the criteria for classification information. This would be a derivative classification based on existing original classification guidance and should be marked accordingly. Source documents for derivative classification markings are normally other classified documents or classification guides issued by agencies with original classification authority. Simply photocopying or otherwise mechanically reproducing classified information is not considered derivative classification.

a. All cleared NARA staff whose duties significantly involve handling classified information are responsible for ensuring that derivative classification is done, when necessary, in accordance with this handbook and the ISOO marking booklet. Observe and respect the classification determinations made by original classification authorities and equity holders. If you believe information has been improperly classified, refer to par. 6.3 regarding challenges to classification.

b. NARA staff who draft any form of documentation that is based on matter that may be classified, including documents prepared in a secure working area, must review the documents to determine the appropriate classification. Documents need to be protected at the highest potential classification level (overall classification of the source) until a determination can be made. Consult equity holders if there is any question regarding the classification of any draft documents or working papers.

c. When information is prepared on classified IT systems, the highest potential classification level is the accreditation level of the IT system. Hard copy output (which

includes paper, microfiche, film, and other media) is not automatically marked at that level, but a classification review must be conducted before releasing the information, or the information must be generated by a software program that has been approved by the accrediting authority for classification reviews. Classification reviews must be performed on human-readable output, and the documents must be appropriately marked, before they may be removed from the system or secure working area.

d. Derivative classifiers must identify themselves in the "Classified By" line of the classification block of the derivatively classified document by name and position. The source document used for the classification of the derivatively classified document, to include the agency and office of origin and the date of the source document, must be cited in the "Derived From" line of the classification block. In derivatively classified documents whose classification is derived from more than one source, the "Derived From" line of the classification block must read, "Multiple Sources," and the list of source documents included in or attached to the document. Declassification instructions taken from the source document, to include a declassification date usually not to exceed 25 years from the date of the source document, must be included in the "Declassify On" line of the classification block. Follow the guidance in section 2 of the ISOO "Marking Classified National Security Information" booklet for further details and examples of proper derivative markings, or consult with your ISPM.

2.3 Inconsistencies in Markings

a. As a rule, documents received from other government agencies that have not been marked to conform to NARA requirements do not need to be remarked. However, documents or series received should clearly indicate a classification level and, if applicable, category or other controlled access information markings.

b. Do not refuse to accept documents, nor return them to the originating agency solely because of improper marking. Instead, contact the sender or your ISPM to resolve any marking issues.

c. When the records were originated by a defunct agency, commission, or committee that has no successor, NARA is responsible for application of any markings, if necessary to clearly indicate the appropriate classification levels and other applicable control markings, but will consult with any equity-holding agencies before applying the markings.

2.4 Declassification Markings

Declassification policy and associated markings are covered in Chapter 6 of this handbook. Authorization to use declassification markings, and the policies and procedures for doing so, are specifically addressed in par. 6.4, including sample markings.

2.5 Markings on Operational Documents

a. Transmittal Documents. Transmittals are documents that have classified documents enclosed with or attached to them and their primary purpose is to convey or introduce the classified enclosure or attachment. The transmittal itself may contain information

classified as high, or higher than the documents transmitted. More often, the transmittal itself is unclassified or classified at a lower level than the transmitted document(s).

(1) If the transmittal contains information classified higher than or at the same level as the documents it is transmitting, mark it as you would any other classified document. If any special warning or control notices are relevant, such as those explained in pars. 2.9 and 2.10 of this handbook, apply them as well to the face of the transmittal document.

(2) If the information in the transmittal document is unclassified or classified at a lower level than one or more of the attachments or enclosures, conspicuously mark the face of the transmittal document as follows:

(a) Top and bottom, with the highest classification found on any of the documents transmitted. For example, if an unclassified transmittal document has one Secret and two Confidential attachments, mark the face of the transmittal document "SECRET."

(b) Show the status of the transmittal document when separated from the classified material. For example, "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES," "UNCLASSIFIED WHEN ATTACHMENT 2 IS REMOVED," "CONFIDENTIAL UPON REMOVAL OF ENCLOSURES," or other similar statements.

(c) Unclassified transmittal documents are not portion marked**.** The marking of classification at the top and bottom of interior pages of a multiple-page unclassified transmittal document is not necessary.

b. Working Papers. Working papers are defined as documents or materials, regardless of the media, that are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information must be dated when created, marked with the highest classification of any information contained in them, protected at that level, and if otherwise appropriate, destroyed when no longer needed. Working papers must be controlled and marked in the same manner prescribed for a finished document at the same classification level when:

(1) released outside NARA by the originator;

(2) retained more than 180 calendar days from the date of origin; or

(3) filed for retention according to the applicable rule in the NARA records schedule.

c. Translations. Translations of U.S. classified information into a foreign language must be marked with the appropriate U.S. classification markings and the foreign language equivalent. They must also clearly show the United States as the country of origin. (See

the Foreign Government Security Classifications chart on the Safety, Security & Emergency page of the NARA@work web site.)

d. Information Transmitted Electronically. Classified information transmitted electronically that is to be retained for the record in operational files, (such as e-mail messages, e-mail attachments in any electronic format, and facsimile (fax) transmissions), must be marked as required for any other classified document, with the following special provisions:

(1) The first item in the text of a classified e-mail message, or any e-mail transmitted over a classified IT system, must be the overall classification of the information. Classified e-mail must never be transmitted over unclassified IT systems.

(2) A properly completed "Classified by" or "Derived from" line, ("Reason," when appropriate), declassification instructions, and downgrading instructions (when appropriate) must be included in the last line of classified e-mail messages. Declassification and downgrading instructions must not be used for information containing Restricted Data (RD) or Formerly Restricted Data (FRD).

(3) Commingling RD or FRD in the same document with NSI classified under E.O. 13526 should be avoided; however, when commingled, the marking requirements for both categories must be followed. The “Declassify On” line will not include a declassification date or event, but will instead be annotated with “Not Applicable (or N/A) to RD/FRD portions” and “See source list for NSI portions.” The source list, as described in 32 CFR Part 2001.22(c)(1)(ii), includes declassification instructions for each source NSI document and will not appear on the front page of the commingled document.

(4) Mark classified fax transmissions as you would any other classified document. The cover page is considered a transmittal document and must be marked according to subpar 2.5a of this handbook. Classified faxes may only be sent or received on secure fax machines.

(5) For information created and printed on an IT system, overall markings and page markings may be applied by that system, provided they stand out conspicuously from the rest of the text.

e. Training Materials. Materials that contain no classified information, but have classification markings applied for training purposes, must also have an accompanying marking which clearly notifies the user that they are actually unclassified. A suitable marking must appear on each page of the document, for example: UNCLASSIFIED - MARKED CLASSIFIED FOR TRAINING PURPOSES ONLY.

f. Files, Folders, and Groups of Documents. Classified files, folders and similar groups of documents must have clear classification markings on the outside of the folder or holder.

A classified document cover sheet (such as Standard Forms 703, 704, and 705, or the applicable SCI or other controlled access information cover sheet) attached to the front of the folder or holder satisfies this requirement. These cover sheets do not need to be attached when the items are in secure storage.

2.6 Markings on Special Media

Materials other than textual paper documents are typically marked with the classification level, or the classification level is made available to holders by another means that clearly conveys the presence of classified information needing protection, such as on transmittals or other accompanying documentation, and on containers, such as boxes or tubes. (See par. 2.3, Inconsistencies in Markings, for additional information.)

a. Blueprints, Maps and Charts. Classified blueprints, schematics, engineering drawings, maps, and charts must have been marked with an overall classification. The classification markings are unabbreviated, conspicuous, and should be located at the top and bottom of the material. The classification should also be included in abbreviated form, within parentheses, following the legend or title. Classification markings must be visible when the item is rolled or folded.

b. Photographs and Negative Film (including aerial imagery)

(1) Photographs and negatives are marked with the overall classification of information they contain. Photographic prints may be marked on the face. The agency may have placed the classification marking on the reverse side. Other marking elements required by E.O. 13526, may have been placed on photographs and negatives, along with the classification marking, or will be included in accompanying documentation.

(2) Roll negatives and positives, and other film containing classified information are marked with their overall classification. This marking is found either on the film itself or on the canister, if one is used. If on the film itself, the marking should be found at the beginning and end of the roll.

c. Slides and Transparencies

(1) Slides and transparencies are marked on the image area of the item and also on the border, holder, or frame, if there is one. Information on the image area of slides and transparencies will be portion marked. Other required security markings may be found in the image area, on the border, holder, or frame, or in documentation accompanying the item.

(2) If a group of slides or transparencies is used and maintained together as a set, each slide or transparency has the overall classification markings on it. The other required security marking elements may be placed on the first slide or transparency in the set, and are not needed on the other slides or transparencies. Slides or transparencies that are permanently removed from a set must be marked as a separate document. If slides or transparencies are

kept in a binder, the binder is marked top and bottom, front and back, and on the spine, to reflect the highest classification level of its contents.

d. Motion Picture Films and Videotapes. Classified motion picture films and videotapes must display embedded warning notices at the beginning and end of the played film/tape that clearly show its highest classification level and are conspicuous to all viewers. Other required security markings are also included at the beginning of the played film/tape. Reels and cassettes must be marked with the overall classification of the item and kept in containers marked with the classification and other required security markings.

e. Sound Recordings. An audible statement announcing the classification should be heard at the beginning and end of sound recordings containing classified information. Reels or cassettes are marked with the overall classification of the item and kept in containers that are also marked with the classification and any other required security markings.

f.Microforms. Microfilm, microfiche, and similar media have their overall classification marked in the image area that can be read or copied. The markings are applied so they are visible to the unaided eye. Other required security markings are also placed on the item or included in accompanying documentation.

g. Information Technology (IT) Systems Storage Media

(1) Removable electronic storage media, e.g., magnetic tape reels, disk packs, diskettes, CDs, DVDs, removable hard drives, disk cartridges, optical disks, magnetic cards, tape cassettes and micro-cassettes, and any other device on which electronic data is stored and is normally removable from an IT system by the user or operator. All removable media containing classified information is conspicuously marked, at minimum, using one of the labels specified in subpar 2.6g(3) below, showing the highest level of classification stored on the device. Follow these marking procedures when creating classified files on new media. If the label is impractical or interferes with the operation of the media, the ISO or cognizant ISPM may approve alternate marking procedures (see subpar 2.6g(4)). Other information normally provided by document markings (e.g., "classified by" and "declassify on" lines) must be available as follows:

(a) If the information is stored in readily accessible format on the device, it does not have to be marked on the outside of the device. For example, if classified files or documents prepared with a word processor are stored on a floppy diskette, and each file bears its own declassification instructions as entered with the word processor, the diskette does not need to be marked with declassification instructions.

(b) If the required information is not stored in readily accessible format on the device, it must be marked on the outside of the device (normally with a sticker or tag) or placed on documentation kept with the device.

(2) Fixed and Internal IT Systems Storage Media. System managers must ensure that IT systems, including word processing systems, provide for classification designation of data stored in internal memory or maintained on fixed storage media in keeping with the guidance in this handbook and NARA 804.

(3) Standard Form (SF) Labels. If not marked otherwise to meet more restrictive security requirements, IT systems storage media and other items covered by this section must be marked with the following labels:

(a) SF 706 - TOP SECRET

(b) SF 707 – SECRET

(c) SF 708 – CONFIDENTIAL

(d) SF 710 – UNCLASSIFIED

NOTE: There is no requirement to use SF 710 in environments where classified information is not created or used.

(4) Press-on sticky labels like the "CD Stomper" should never be used as delimitation of the optical disc will occur. Keep in mind that CD-R discs are not considered a long term storage medium; however, any labeling that is to be applied to an optical disc with an oil-based marker such as a "Sharpie" should only be marked on the inside ring, not where the data is recorded. Ideally, an optical media-safe water-based marker with permanent qualities should be used when labeling optical media.

2.7 Document Reference Markings

When references are included as part of a classified document, each document referenced or listed should clearly reflect the classification of the document listed by using portion markings. Hypothetical examples citing classified references:

a. When the document is classified, but the title or subject is not:

(U) NARA Directive 123-45, Marking References or Bibliographies, March 23, 2003, Secret.

b. When the document AND the title or subject are both classified:

(C) NARA Directive 123-45, Marking References or Bibliographies, March 23, 2003, Secret. (for a Confidential title, Secret document)

(TS) NARA Directive 123-45, Marking References or Bibliographies, March 23, 2003, Top Secret. (for a Top Secret title, Top Secret document)

2.8 Legacy Executive Order Classification Markings

Archival records in NARA's legal custody may contain markings that were prescribed in previous executive orders dealing with the protection of classified information. Examples of these legacy markings are as follows:

a. RESTRICTED

The RESTRICTED marking for classified information originated by the United States was eliminated by E.O. 10501. All information marked as "RESTRICTED" has been automatically declassified unless the owning agency took specific steps to exempt that information from declassification. If exempted, the records were required to be re-marked with an appropriate current classification category marking (Confidential, Secret, or Top Secret).

NOTE: This marking and the associated information it designated is separate and unrelated to the markings established under the Atomic Energy Act of 1954, as amended, (i.e., RESTRICTED DATA/FORMERLY RESTRICTED DATA).

b. GROUP Markings

E.O. 10501, as amended by E.O. 10964, dated September 20, 1961, organized classification into four groups, each of which contained declassification instructions. However, each group is now subject to downgrading and automatic declassification in accordance with E.O. 13526. These group markings may appear on documents and material in NARA custody. The groups consist of:

(1) Group 1. Information originated by foreign governments or international organizations and over which the United States government has no jurisdiction, information, provided for by statutes such as the Atomic Energy Act, and information requiring special handling, such as intelligence or cryptography. This information was initially excluded from automatic downgrading or declassification.

(2) Group 2. Extremely sensitive information that the head of the agency or his designees initially sought to exempt, on an individual basis, from automatic downgrading and declassification.

(3) Group 3. Information that warranted some degree of classification for a then indefinite period. Such information was to be automatically downgraded at 12 year intervals until the lowest classification was reached, but was not to be automatically declassified.

(4) Group 4. Information that did not qualify for, or was not assigned to, one of the first three groups. Such information was to be automatically downgraded at three-year intervals until the lowest classification was reached, and was to be automatically declassified twelve years after the date of issuance if it had not already occurred.

2.9 Foreign Government Information Markings

a. Foreign Government Information (FGI) is defined in E.O. 13526 as:

(1) information provided to the United States government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, must be held in confidence;

(2) information produced by the United States government pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor executive order.

b. FGI may retain its original country markings, but the receiving U.S. agency may indicate the equivalent U.S. classification and country of origin in English. Refer to the Foreign Government Security Classifications chart on the Safety, Security & Emergency page of the NARA@work web site. It shows foreign classifications which may be found on documents in NARA holdings. Derivatively classified documents containing FGI should exhibit U.S. as well as foreign classification sources. Other markings that may appear on documents containing FGI include:

THIS DOCUMENT CONTAINS
(COUNTRY OF ORIGIN) INFORMATION

or

THIS DOCUMENT CONTAINS (NAME OF COUNTRY AND FOREIGN CLASSIFICATION LEVEL) INFORMATION TO BE TREATED AS (U.S. EQUIVALENT CLASSIFICATION) – MODIFIED HANDLING AUTHORIZED

or

THIS DOCUMENT CONTAINS
FOREIGN GOVERNMENT INFORMATION

c. Documents containing FGI are usually portion marked using the accepted country code (see subpar 2.10b(3)(g) of this handbook), along with the abbreviation for the U.S. classification level. For example, FGI from Great Britain at a classification equivalent to U.S. Secret information would be portion marked "GBR-S." If the source country cannot

be revealed, the page marking in the third example above would be used, and the portion marking would contain the acronym FGI along with the abbreviation of the U.S. classification level (e.g., FGI-S).

2.10 Controlled Access Information Markings

In addition to classification markings prescribed by E.O. 13526 and previous executive orders, the warning notices or caveats described below may appear on documents in NARA's custody:

a. Restricted Data/Formerly Restricted Data. The Department of Energy (DOE) is responsible for policy and guidance on Restricted Data (RD) and Formerly Restricted Data (FRD). RD and FRD is governed by the Atomic Energy Act of 1954, as amended, and is handled, protected, and controlled in accordance with DOE Order 471.6, Information Security, and Title 10, Code of Federal Regulations, Part 1045 (10 CFR Part 1045), Nuclear Classification and Declassification.

(1) Restricted Data. The Atomic Energy Act of 1946 established RD, which deals with nuclear weapons and related technologies. RD is defined as all data containing the:

(a) design, manufacture, or utilization of atomic weapons,

(b) production of special nuclear material, or

(c) use of special nuclear material in the production of energy. Records or documents containing RD, as defined in the Atomic Energy Act, are marked as follows:

RESTRICTED DATA
This material contains restricted data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

(2) Formerly Restricted Data. The Atomic Energy Act was revised in 1954, allowing information concerning the utilization of nuclear weapons to be trans-classified to another category known as Formerly Restricted Data. The Department of Defense (DoD) and DOE have joint authority for decisions concerning FRD. FRD is defined as classified information that has been removed from the RD category and relates primarily to the military utilization of atomic weapons. Records or documents containing Formerly Restricted Data (FRD), as defined in the Atomic Energy Act of 1954, , as amended, are marked as follows:

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative and criminal sanctions.
Handle as Restricted Data in foreign dissemination.
Section 144.b, Atomic Energy Act, 1954.

(3) Sigma. Most RD/FRD documents in NARA holdings will consist of obsolete access levels - designated as Sigma levels 1 thru 13. These Sigma levels have been used for many years and may remain marked on legacy documents, or they may not have any special markings. Documents marked as being Sigma 14, 15, 18 or 20 involving nuclear weapons data and design, are considered Sensitive Use Control Information (SUCI) and are highly restricted similar to Sensitive Compartmented Information (SCI) or Special Access Program (SAP) information as described in subpars 2.10b & c below.

(4) Transclassified Foreign Nuclear Information (TFNI). Under a process called "transclassification", as permitted under 42 U.S.C. 2162(e), the DOE and the Director of National Intelligence may jointly remove information concerning the atomic energy programs of other nations from the Restricted Data category, which they determine necessary to carry out the provisions of 50 U.S.C. 403 and 403–1, and can be safeguarded under E.O. 13526 as classified national security information.

(a) When Restricted Data information is transclassified and is safeguarded as classified national security information, it must be handled and protected according to the provisions of E.O. 13526 and this handbook. Such information is labeled as ''TFNI'', with any additional identifiers prescribed by DOE. The label ''TFNI'' must be included on documents to indicate the information's transclassification from the Restricted Data category and that its declassification process remains under the authority of DOE, in accordance with the Atomic Energy Act.

(b) Automatic declassification of documents containing TFNI is prohibited. Documents marked as TFNI are excluded from the automatic declassification provisions of E.O. 13526. If DOE determines that a TFNI designation may be removed, any remaining information classified under E.O. 13526 must be referred to the appropriate equity owning agency in accordance with the declassification provisions of E.O. 13526 and this handbook.

b. Sensitive Compartmented Information (SCI). Documents and material belonging to the SCI control system have unique markings and contain information of the most sensitive nature. SCI programs are established and administered by the Director of National Intelligence (pursuant to the Intelligence Reform and Prevention of Terrorism Act of 2004). The governing directive is Intelligence Community Directive (ICD) 703, Protection of Classified National Intelligence Including Sensitive Compartmented Information. There are three SCI control systems: SPECIAL INTELLIGENCE (SI), also referred to as Communications Intelligence (COMINT), TALENT KEYHOLE (TK), HUMINT CONTROL SYSTEM (HCS), and one subsystem: GAMMA (G).

(1) A previous control system, BYEMAN (B), was eliminated on May 20, 2005. The code word BYEMAN and its trigraph BYE are now unclassified and are no longer valid markings; however, the information contained in these documents remains classified as SCI and has been transferred into the TK control system. Handle all such information as "TK" when it is pulled for review. When transmitted to other agencies, the transmitted copy must be re-marked as TK.

(2) SCI document markings include the standard classification levels associated with these control system names or abbreviations. Examples of this would be: TOP SECRET//HCS or TOP SECRET//SI/TK/G. Sometimes a code word may also be used, which itself is usually classified. Code words previously used by the National Security Agency (NSA), such as UMBRA, SPOKE, MORAY, and ZARF, were discontinued as of October 12, 1999; however, they may still be seen on documents in NARA holdings. Records marked under eliminated or discontinued control systems remain classified and require continued protection until properly declassified.

(3) Dissemination Control Markings. Documents associated with the intelligence community that may be found in NARA's custody can bear the following markings which were, or are, used for the dissemination of intelligence information to ensure adequate protection for intelligence purposes while facilitating access:

(a) WARNING NOTICE—Intelligence Sources or Methods Involved (WNINTEL). WNINTEL is an older warning notice concerning intelligence information that has been superseded by the markings listed below. WNINTEL appears on older documents in NARA holdings.

(b) NOT RELEASEABLE TO CONTRACTORS/CONSULTANTS (NOCONTRACT). This older marking indicates that a document or material contains information that cannot be shared with contractors. It has been superseded by the PROPIN marking (see subpar 2.10b(3)(f) below).

(c) U.S. ONLY. This older marking indicated that a document contained information releasable to U.S. citizens only. It may appear in documents in NARA holdings.

(d) NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN). This marking indicates that the document or material contains information that is not to be disclosed to non-U.S. citizens. For portion marking NOFORN is abbreviated NF.

(e) DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON). ORCON is the most restrictive of the intelligence community markings, which is an

indication of the high sensitivity of the information. For portion marking ORCON is abbreviated OC.

(f) CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN). Documents marked PROPIN contain information that cannot be released to any individual or organization outside the Federal government without the permission of the originator. For portion marking PROPIN is abbreviated PR.

(g) AUTHORIZED FOR RELEASE TO COUNTRY (REL TO). Documents marked REL TO indicate that the originator has authorized the release of embedded intelligence information to the country or countries indicated. The countries are identified by the International Organization for Standardization three-letter country code (GBR-Great Britain, DEU-Germany, etc.) available on the United Nations Statistics Division web site.

c. Special Access Program (SAP) Information. Special access programs are established under authority of section 4.3 of E.O. 13526. The Secretaries of State, Defense, Energy, Homeland Security, and the Director of National Intelligence, or the principal deputy of each, and otherwise as directed by the President, may establish and maintain Special Access Programs (SAPs) when necessary to protect the Nation's most sensitive and critical information or when required by statute.

(1) There are three types of SAPs: acknowledged, unacknowledged, and waived.

(a) Acknowledged Special Access Program. A SAP that is, or has elements that are, publicly acknowledged to exist and whose purpose is identified (e.g., the B-2 or the F-117 aircraft program) while the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is generally unclassified. Members of applicable Congressional oversight committees are briefed on these types of programs.

(b) Unacknowledged Special Access Program. The existence of this type of SAP, and each element within it, is classified information; and, the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is often unacknowledged, classified, or not directly linked to the program. Members of applicable Congressional oversight committees are briefed on these types of programs.

(c) Waived Special Access Program. A SAP for which the originating Department Secretary or agency head (i.e., Secretaries of State, Defense, Energy, and Homeland Security, or the Director of Central

Intelligence) has waived the applicable reporting requirements of Title 10, United States Code, Section 119 (10 U.S.C. 119), or 50 U.S.C. 2426, is designated as a "Waived" program and, therefore, has more restrictive reporting and access controls. Access is extremely limited. In Congress, only the Chairman and the Senior Minority member (and by agreement, their staff directors) of applicable oversight committees may be briefed on waived programs.

(2) SAP information requires additional control and protective measures beyond those normally required for other classified information at the same classification level. Markings on SAP information include the overall classification level, and should include the caveat "Special Access Required," (SAR) and a code word or nickname (also expressed as a two- or three-letter digraph or trigraph) that is associated with that particular program. Portion markings would look like "(TS/TRO)," and a typical example of an overall page marking would be:

TOP SECRET // SPECIAL ACCESS REQUIRED // TIMES ROMAN

or

TOP SECRET/SAR/TRO

d. North Atlantic Treaty Organization (NATO) Information. Documents containing classified NATO information are protected by treaty from disclosure. Documents marked COSMIC are NATO's equivalent of Top Secret. NATO documents that contain RD/FRD-equivalent information are marked ATOMAL. NATO documents bear the NATO marking preceding any Secret or Confidential markings. Portion marking of documents containing NATO Secret or Confidential information have the abbreviated form (NATO-C or NATO-S), while documents containing Top Secret information are abbreviated (COSMIC-TS). Classified NATO documents must be handled and controlled according to United States Security Authority for NATO Affairs (USSAN) Instruction 1-07, Implementation of NATO Security Requirements. NATO security classifications and their significance are:

(1) COSMIC Top Secret (CTS) unauthorized disclosure would result in exceptionally grave damage to NATO.

(2) NATO Secret (NS) unauthorized disclosure would result in grave damage to NATO.

(3) NATO Confidential (NC) unauthorized disclosure would be damaging to NATO.

(4) NATO Restricted (NR) unauthorized disclosure would be detrimental to the interests or effectiveness of NATO. This category of NATO information does not correspond to an equivalent U.S. classification level, but must be

handled in accordance with USSAN 1-07 and this handbook in the same manner as U.S. Confidential information.

(5) NATO Unclassified is a marking applied to NATO information that does not require security protection. It is generally handled the same as U.S. unclassified information except when requested by a non-NATO nation, organization or individual. In these cases a decision must be made as to whether release would harm the interests of the North Atlantic Treaty Organization. Refer these to the equity holder(s) for their determination.

e. Other Warning Notices. There are other warning notices in current use or in documents that NARA maintains in its holdings, such as:

(1) Communications Security (COMSEC). COMSEC documents or materials are marked according to Committee on National Security Systems Instruction (CNSSI) 4002, Classification Guide for COMSEC Information. This is a classified document, so please see the ISO if you need to review or obtain a copy.

(2) Special Category (SPECAT). Documents containing SPECAT information are rated as Top Secret, Secret, or Confidential and have a name associated with the special category. For portion marking, SPECAT is abbreviated SC.

(3) Single Integrated Operations Plan (SIOP). Documents containing SIOP information are extremely sensitive as they reveal details of U.S. war planning. SIOP information is normally classified Top Secret. For portion marking, SIOP is the abbreviation used.

(4) Dissemination and Reproduction Notices. Classified information that is intended for limited dissemination or reproduction, or both, must have a statement or statements on its cover sheet, first page, or in the text, substantially as follows:

REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR OR HIGHER AUTHORITY

FURTHER DISSEMINATION ONLY AS DIRECTED BY (OFFICE OR OFFICIAL) OR HIGHER AUTHORITY

NOTE: Limited Dissemination (LIMDIS) is no longer an actively used marking for classified information, though it may appear on accessioned documents. Under the Controlled Unclassified Information (CUI) program, this term refers to any marking approved by the CUI Executive Agent intended to restrict access to and dissemination of unclassified information by or to certain individuals, organizations, or other identifiable group(s). See

Chapter 4 of this handbook for more information on reproduction and safeguarding classified information.

(5) Other Notations. Other notations or restrictions may be found on documents in NARA custody. Consult with the originating or responsible agency when notations of unknown meaning are found on documents.

2.11 Unmarked Classified Information

In addition to marked classified information, records such as Presidential papers, documents pertaining to the national defense or foreign relations of the United States, donated papers, other historical documents, or even handwritten notes may contain classified information that has not been appropriately marked or identified, but is nonetheless subject to the provisions of E.O. 13526. Categories of information classified by agencies with original classification authority (OCA) are found in section 1.4 of E.O. 13526. Please consult the equity holders or see your ISPM if you are unsure about the classification of any information.

a. The following terms or topics in an unmarked document may indicate that it contains unmarked classified information. Documents with these terms may need to be safeguarded until the agency of primary equity conducts a classification review.

b. This is not an all-inclusive list of terms, but may serve as a guide to indicate the possibility of unmarked national security information:

Intercept; clandestine; covert; controlled source; confidential source; Controlled American Source (CAS); references to Station Chief, “the Agency”, National Intelligence Estimate (NIE); information from “intelligence” or from “our agent”; yields; kiloton; abbreviations for megaton and kiloton (MT and KT); satellites used for intelligence purposes; lists of weapon systems or detailed information on weapons; detailed correspondence with or about a foreign government, or from a Head of State; many NATO or SEATO (now defunct Southeast Asian Treaty Organization) documents; Roger Channel, and any documents from the President’s Foreign Intelligence Advisory Board.

[Return to TOC]

Chapter 3

ACCESS

3.1 Access to Classified Information

This chapter addresses the procedures and requirements for obtaining and providing access to classified information. Access is the ability or opportunity to gain knowledge of classified information. An individual may gain access to classified information by simply being in a location or facility where such information is maintained, if adequate security measures are not followed. There are many reasons why a person may need access to classified information at NARA: e.g., preservation and holdings maintenance; declassification review; ongoing business of the President; criminal or civil law enforcement investigation; privilege review by former Presidents or their representatives; historical research by agency historian or former official. And there are numerous authorities controlling access, including E.O. 13526, E.O. 12968, Access to Classified Information, the Presidential Records Act, and the Presidential Recordings and Materials Preservation Act. However, no person is entitled to access to classified information based solely on the basis of pay grade, position, or security clearance.

a. An individual may have access to classified information only if that person:

(1) holds a security clearance at or above that of the classification level of the information to be viewed;

(2) is engaged in legitimate government business;

(3) has a need to know (cannot reasonably fulfill their appointed duties without access); and

(4) has been given initial security training as described in Chapter 8 of this handbook, a SF 312 briefing and completed the required SF 312, Classified Information Nondisclosure Agreement, and also any controlled access agreements, as appropriate, which may be verified through the Security Management Division (BX).

NOTE: A list of security access briefing and debriefing forms may be found in par. 3.14 of this handbook.

b. Whenever reviewing classified information in a research room, all individuals must read and sign NA Form 14128, Notice to Users of NARA Classified Research Rooms, before being given access to the information.

c. Employees and contractors of government entities other than NARA must provide written proof to BX in the form of a Visit Authorization Letter (VAL), through their security office, documenting that they meet the access requirements of subpar 3.1a. See subpar 3.3b for further information on the VAL.

d. Regardless of clearance level and need to know, individuals must continue to meet the personnel security standards listed in section 3.1 of E.O. 12968.

e. Additional restrictions to access for reasons other than national security are addressed in 36 CFR Parts 1256 and 1270, E.O. 13489, the Federal Records Act (44 U.S.C. 2108 note), the Presidential Records Act (44 U.S.C. 2201-2209), the Presidential Recordings and Materials Preservation Act (44 U.S.C. 2111 Note), or the donor's deed of gift for any donated collection being accessed. All requests for access should be maintained under items 258, 1415 through 1422, or 1470 of the NARA Records Schedule, as applicable.

3.2 Distinguishing among Access, Clearance and Need to Know

a. Access should be thought of as the permission to view or handle classified information, which individuals holding the information may give to other individuals, but may only be given to persons with both a clearance and a need to know.

b. A clearance is a certification from an agency's security officials that a person has been investigated and deemed trustworthy enough to be given access up to a specific classification level, when needed (see NARA 273, Collateral Security Clearances).

c. Need to know is established when the holder of the classified information can identify individuals or organizations within the executive branch requiring access to classified information in order to perform their official duties in an authorized governmental function. This may be done through one-on-one determinations, interagency agreements, information sharing directives, or other designations consistent with section 4.1(a) of E.O. 13526 and par. 3.1a. of this handbook. Access to classified information is not granted automatically to state or local governments or to other branches of the Federal government, such as Congress.

d. Special access, or controlled access, is an agency-level authorization, granted to individuals who have a clearance, need to know, and meet additional trustworthiness standards, allowing them access to categories of classified information (e.g., SCI, RD/FRD, SAP information) employing security control measures exceeding that required for other forms of classified information.

3.3 Responsibility for Determining Access

a. The NARA employee authorized to have possession, knowledge, or control of classified information, and not the prospective recipient, exercises the final responsibility for verifying:

(1) whether the recipient's official duties require access to classified information; and

(2) through BX, whether the recipient has been granted the appropriate security clearance by proper authority.

NOTE: This principle is equally applicable to NARA employees, other Federal agencies, contractors or foreign government officials.

b. Determining and verifying the appropriateness of proposed access by other agency personnel, contractors, or non-government researchers requires coordination among the legal custodian of the records, the equity holders, and any parties with statutory authority. If NARA offices have any questions on eligibility for access to classified information at NARA, they should contact BX. The following procedures must be followed for non-NARA persons to obtain access to classified information:

(1) Security clearances must be passed with a Visit Authorization Letter (VAL), which must be received at NARA for anyone coming to access or discuss classified information. BX will maintain the VALs and keep a database list of all visitors to NARA who have a VAL on file. The NARA sponsoring office should determine whether the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. Establish positive identification, appropriate clearance, and need-to-know by coordinating with BX to ensure visitors have a VAL on file that has not expired prior to disclosure of any classified information. Visitors must only be afforded access to classified information consistent with the purpose of their visit.

(2) Visitors must send their VAL directly from their agency security office to BX. At a minimum, the VAL must contain the visitor's:

(a) name, social security number, date and place of birth, and citizenship;

(b) organization name, address, and telephone number;

(c) personnel security clearance level (and access if applicable, e.g., SCI, Q) and the date it was granted;

(d) last investigation date and type;

(e) NARA point of contact and purpose of the visit; and

(f) inclusive dates of the visit, i.e., the period during which the VAL is to be valid. (In the case of a contractor, this period cannot exceed the term of the current contractual arrangement. If there is a contractual arrangement, the name, number, and expiration of the contract must be included. If there is no contractual arrangement, that fact must be clearly indicated.)

(3) NARA staff planning to visit another organization for a similar purpose must contact BX at least 5 workdays in advance of their visit to pass their clearances. BX prepares the VAL.

(4) Government representatives acting in official capacities as inspectors, investigators, or auditors may visit NARA facilities by presenting appropriate government credentials upon arrival, in lieu of a VAL; however, it does not authorize them access to classified information. If such access is necessary, their agency must provide a VAL before access may be given.

3.4 Access by Government Officials or Contractors of Transferring Agencies

Government officials and contractors representing a Federal agency, commission, or committee that transferred legal or physical custody of classified information to NARA may have access to the information, if they meet the requirements of par. 3.1.

3.5 Access by Government Officials or Contractors of Non-Originating Agencies

a. Records in NARA's Physical, but Not Legal, Custody:

(1) Access by government officials and contractors representing Federal agencies, commissions, or committees, to classified information originated and transferred to NARA's physical custody by a different agency, is permitted:

(a) when BX receives written authorization from the originating or transferring agency; and

(b) if the requirements of pars. 3.1 and 3.3 are met.

(2) Incumbent Presidential records containing classified information are held in courtesy storage and controlled by agreement between the Office of Presidential Libraries and the White House.

(3) Congressional records (those of the U.S. House of Representatives and the U.S. Senate) in NARA's physical custody are subject to the rules of their respective chamber (44 U.S.C. 2118). Under these rules, the Office of the House Clerk and the Office of Senate Security, on behalf of the originating committee, can request the loan of original classified records in NARA's physical custody for use by the committee that created the documents.

b. Records in NARA's Legal Custody:

Access to classified information in NARA's legal custody by government officials representing non-originating agencies is permitted for purposes of declassification review, upon written authorization from the agencies holding the primary equities or when applicable under the Interagency Agreement on Access for Official Agency Historians. All persons must meet the requirements of pars. 3.1 and 3.3.

(1) Requests for access to classified Presidential records and Nixon Presidential Historical Materials are governed by the Presidential Records Act (PRA)

and the Presidential Recordings and Materials Preservation Act (PRMPA), and their implementing regulations, respectively.

(2) Requests for access to donated historical materials or accessioned Federal records in the custody of the Presidential libraries, such as Presidential commissions, must be submitted directly to the director of the library or the materials staff holding the records.

(3) Requests for access by representatives of agency historical offices (e.g., the Department of State Office of the Historian, for use in such official government publications as the "Foreign Relations of the United States"), must be submitted to the National Declassification Center (NDC) for Federal Records, and to the appropriate Presidential library or Presidential Materials Division (LM) for Presidential records or materials.

(4) Requests for access to all other classified Federal records, including by inspectors, investigators, or auditors, must be submitted to the NARA General Counsel (NGC), except as noted in subpars 3.5b(2) and (3) above, specifying the records requested and the purpose of the request. NARA only accepts requests:

(a) from a senior agency official (i.e., agency head, deputy agency head, office or division head or deputy);

(b) from the chairman of a Congressional committee or subcommittee that originated or has jurisdiction over the information requested (classified information that may be subject to Executive privilege may not be released to legislative branch officials without consulting NGC); or

(c) by a court order signed by a Federal judge or a criminal grand jury subpoena if the request involves judicial proceedings.

NOTE: When requests are received from any party involved in a prosecution under the Classified Information Procedures Act (18 U.S.C. Appendix 3), NARA requires that the authorization for access to classified information in NARA's custody be obtained from the equity holders by the Department of Justice in accordance with the governing statutory authorities.

(5) Upon notification from NGC that a request has been properly made, the unit with custody of the records contacts the requester and arranges for review of the specific documents.

(6) If a Federal agency or Congressional committee wishes to publicly release any classified information to which it has gained access through the above procedures, it must request declassification of the information directly from each agency equity holder. Once declassification has been approved, the

Federal agency or Congressional committee must follow the release provisions of their access letter(s) and notify NARA before releasing the information.

NOTE: Any additional statutory requirements other than those required for classification must also be met.

3.6 Access by the Incumbent President or Vice President

Access by the incumbent President, Vice President, or their designated representatives to classified Presidential or Vice Presidential materials created in previous administrations is handled as follows:

a. Executive Privilege Reviews. As stated in par. 3.7, the provisions of the Presidential Records Act and E.O. 13489 govern access to Presidential records. The incumbent President or a designated representative will have access to these materials for the purposes of conducting privilege reviews should the President request such access, subject to subpar 3.9d, for access by non-government researchers performing PRA production reviews or historical research, as appropriate.

b. Ongoing Government Business. Incumbent Presidents, Vice Presidents or their designated representatives will have access to the materials of former administrations for the purpose of ongoing government business.

3.7 Access by Former Presidents and Vice Presidents

Access by former Presidents, Vice Presidents, or their designated representatives to classified Presidential or Vice Presidential records or donated historical materials created during their administration.

a. Executive Privilege Reviews. Any access to Presidential or Vice Presidential records created after January 20, 1981 is subject to the terms and provisions of the Presidential Records Act (44 U.S.C. 2201-2209) and the notification procedures under E.O. 13489 and 44 U.S.C. 2208. Former Presidents, Vice Presidents or their designated representatives will have access to these materials for the purposes of conducting privilege reviews should they request such access, subject to 44 U.S.C. 2204(f) and subpar. 3.9d, on access by non-government researchers performing PRA production reviews or historical research, as appropriate.

b. Research. Former Presidents, Vice Presidents or their designated representatives will have access to the materials of their administrations for research or reference purposes in accordance with 44 U.S.C. 2204, subject to 44 U.S.C. 2204(f) and subpar. 3.9d for access by non-government researchers performing PRA production reviews or historical research, as appropriate.

c. Additionally, former Presidents and Vice Presidents may be afforded access to classified information in accordance with section 4.4 of E.O. 13526.

3.8 Access by Former Presidential and Vice Presidential Appointees

Individuals who occupied policymaking positions to which they were appointed by the President or Vice President may have access to classified information they originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee. See section 4.4 of E.O. 13526. Access is conditioned upon:

a. the individual meeting the access requirements of par. 3.1; and

b. written authorization transmitted directly from the originating agency to NARA, or

c. other statutory authorities or deeds of gift that may afford access.

NOTE: For procedures to be used in serving materials once access conditions are met, see subpar 3.9d, on access by non-government researchers performing production reviews per the Presidential Records Act (PRA) or historical research.

3.9 NARA Research Room Procedures for Accessing Classified Information

General guidance for using NARA research rooms is located in 36 CFR Part 1254. This section may be used to form the basis of Standard Operating Procedures (SOPs) for classified research rooms, including for agency officials and their contractors, non-government researchers, and NARA employees. NARA staff must prepare classified research rooms for use by appropriately authorized researchers. NA Form 6052, Checklist for Classified Visits and Meetings, should be used for this purpose (see par 4.11 of this handbook).

a. Access Control. Researchers who meet the access requirements specified in this chapter may be allowed access to classified information. Access is controlled for all types of classified information, regardless of the legal status (e.g., accessioned records, all records center holdings regardless of disposition, Presidential records, and donated historical materials). The following procedures apply to classified research rooms:

(1) At the first visit, NARA staff must verify the researcher's security clearance and two (2) forms of identification: a government-issued photo ID, such as a driver's license, and

(a) a NARA research card; or

(b) an agency badge if conducting official business, by examining unaccessioned materials (e.g., at an FRC), etc..

(2) All researchers must complete NA Form 14128 and sign-in on a visitors log, as described in par. 4.10c(3)(b). The visitor log is maintained within the research room and is retained for two years in accordance with NARA records schedule, item 650-2.

(3) Limit the research of classified information to a designated classified research room if the volume of research at the facility justifies the establishment of such a room.

(4) If the facility does not have a designated classified research room, use a Sensitive Compartmented Information Facility (SCIF), other secure facility, or controlled area, as appropriate. If the information is SCI or SAP, it may only be reviewed inside a SCIF or SCIF-accredited classified research room or an accredited temporary SCI secure working area (TSWA). Never allow researchers to review classified information in an open office. When using a dedicated conference room or other controlled area (rooms or offices to which access can be controlled or restricted by cleared staff, locked doors and covered windows), follow the guidance in subpar 4.11b.

(5) NARA staff, acting as monitors in the research room, must have the appropriate clearances for the records under review. If SCI can only be stored within the research room because of space limitations, it must first be accredited as a SCIF. Individuals opening or closing a SCIF are required to have SCI access and must remain in the SCIF while it is open.

(6)Do not provide access to authorized researchers in any research room where unauthorized researchers or staff not cleared at the appropriate level are present.

(7)Researchers must be restricted from any room or records holding area that holds records other than those to which they have due access authority, unless waived by the Deputy Archivist.

b. Clean Room Procedures. Clean research room procedures must be strictly enforced. When entering the classified research room, all researchers are required to present any papers, notes, or written materials to the research room monitor to be checked:

(1) If researchers have more than one page, the room monitor staples the pages together and marks them on the back of the last page to indicate that they were brought into the research room by the researcher. All subsequent notes must be taken on NARA-provided letterhead or otherwise identifiable stationery. Note paper and pencils are available for researcher use in the research room.

(2) All notes created during research from classified information and classified reproductions must be protected at the level of the information from which the notes were taken. Researchers may not remove such notes or copies from NARA unless authorized by the equity holder (see subpar 3.9e). Using NARA's derivative classification authority, stamp such notes with the appropriate classification markings or refer them to the equity-holding agency for review and appropriate classification marking. Pay particular attention to any controlled access restrictions that may apply to any of the reproductions. When release to researchers is not authorized under subpar 3.9e, the notes must be transmitted to the equity holder, if they request, or

directly to the researcher's or contractor's sponsoring government agency for further handling.

(3) The following items are prohibited within the classified research room: briefcases, boxes, satchels, valises, purses, day packs or other large containers, overcoats, raincoats, hats or similar apparel.

(4) The following items are permitted in the classified research room: wallets, coin purses, keys, credit card/identification holders, and official courier briefcases or pouches when authorized (see subpar 3.9e(1)).

(5) The use of Portable Electronic Devices (PEDs) in classified research rooms are restricted as described in par. 4.13.

(a) Government-owned classified laptops are authorized for use in SCIFs if configured and accredited in accordance with ICD 503, Information Technology Systems Security Risk Management, Certification and Accreditation.

(b) Personally-owned laptops are prohibited in classified research rooms at all times. NARA may provide researchers with laptops configured to mitigate security concerns, when necessary and available. The researcher's use of a NARA laptop and associated media must be sanctioned in the access letter from the equity holder. The researcher must save all notes to previously unused "factory fresh" removable media (e.g., CD, DVD or thumb drive) provided to them by NARA staff. Researchers must return the media to the room monitor before leaving the classified research room. NARA sends the media to the equity holding agency for review. The laptop must also be returned to the research room monitor.

c. Providing Classified Information for Research. Researchers may only review classified documents pursuant to the stipulations in their access letter from the equity holder in accordance with all statutory requirements governing the records. Procedures for control and management of classified records provided to researchers may vary by location and outlined in local SOPs.

(1) Use the Holdings Management System (HMS) to ensure accountability and control of classified records at Archives II through the use of HMS-generated work requests, providing a process to produce, handle, and audit records "pull slips" needed to remove and return records to and from the classified stacks. Follow the records pull procedures outlined in NDC Standard Operating Procedure #10.

(2) If you use the NA Form 14001, Reference Service Slip, follow the procedures outlined in your local SOPs or as follows:

(a) White Copy. The staff member bringing the records to the classified research room must sign and date in the lower left-hand corner of the form as a record of their actions. Keep all white copies on file for a period of two years, in accordance with NARA records schedule, item 1420-2.

(b) Pink Copy. The researcher must sign and date the front of this copy. On the reverse side, the researcher must also enter the date, time, and initials when charging out records. This procedure is repeated when the documents are returned or charged out again. Hold the pink copy in the Researcher Request box located in the research room. Once the researcher has finished using the records, pull the pink copy from the Researcher Request box and attach it to the records, indicating that they can be re-filed. After re-filing the records, return the pink copy to the research room for filing in accordance with NARA records schedule, item 1420-1 or 1470, as applicable.

Green Copy. This copy must remain attached to the requested boxes at all times while in use. It may be destroyed once the boxes are returned to their permanent location.

Yellow Copy. At the time the staff member removes a container of records from a stack shelf or drawer, the yellow copy must go in the container's place to indicate that records have been removed. When the container is re-filed in its proper place, the yellow copy may be destroyed.

(3) When other NARA-approved reference service forms are used, units must adequately document chain of custody and prescribe the use of such approved forms in Standard Operating Procedures.

(4) If the researcher requires additional records not already available in the research room, the room monitor must call the designated support staff to retrieve the documents. The room monitor must not leave the research room while researchers or classified documents are present.

(5) Provide the researcher with only one box of records at a time. Multiple boxes may be pulled and made ready for use but researchers may have only one box on the table at a time. Boxes that are waiting to be used must be monitored by NARA staff cleared at the appropriate level.

(6) Ensure that researchers complete the approved reference service form as each box is provided.

(7) Monitor researchers continuously during their use of records. Whenever necessary, limit the number of researchers or make more staff members available to facilitate adequate monitoring.

(8) When possible, implement secure, overt closed-circuit television (CCTV) monitoring and recording. Use the CCTV system continuously during the use of records to act as a deterrent and to aid an investigation, if necessary.

d. Additional procedures for access by non-government researchers performing special access production reviews or historical research.

(1) NARA staff must ensure that the room and any researchers are continuously monitored by a NARA staff member cleared at the appropriate level.

(2) NARA staff must provide only numbered copies, unless a waiver has been granted for review of original documents (see subpar 3.9d(5) below). Number the pages of the copies sequentially, starting with page 1 of the first document through the last page of the last document.

(3) NARA staff must maintain a log (with description and page counts of the individual documents) or a second control set of all documents provided. The original documents may be used as the second control set.

(4) The researcher must sign NA Form 14001 or other approved reference service form when prescribed by local Standard Operation Procedures. The signed form serves as a receipt for each box provided. Returned boxes must be reviewed by NARA staff before the researcher leaves the classified research room. When available, a second NARA staff member may review the returned documents while the first staff member monitors use of another box by the researcher.

(5) Access to original records, rather than numbered copies may be waived, except as described in subpar. 3.9d(5)(b).

Waiver for the Original Documents Instead of Copies. Requests to use original documents must be sent in writing, to the appropriate ISPM, justifying the need for original documents and affirming they understand that NARA employs double monitoring during original document reviews. The ISPM sends the request, along with time requirements and likely production quantities, to the NGC, appropriate NARA office executive and the Senior Agency Official (SAO) to evaluate the factors in the request and recommend whether to grant a waiver. NGC sends the request and recommendation to the Deputy Archivist for the final decision. The location providing access is responsible for maintaining double coverage (two dedicated monitors) in the classified research room whenever researchers are allowed to use original documents.

Exception to Waiver for the Original Documents Instead of Copies. In accordance with 44 U.S.C. 2204(f), access to original records may not be provided to any individual serving as a designated representative to a former President, if that individual has been

convicted of a crime relating to the review, retention, removal, or destruction of records of the Archives.

e. Agency Researchers Authorized to Courier Classified Information. Researchers designated by their own agency as an official courier may receive copies of classified documents to take with them only in accordance with the access letter(s) from the equity holder(s) and any other statutory requirements governing those records.

(1) If a researcher needs to take copies of classified documents with him or her, he or she must produce a valid courier badge, or memo on official letterhead from their agency, granting permission to transport classified information at the classification level of the documents. If the researcher has a lockable courier pouch or briefcase, NARA staff prepares the initial wrapping (inner envelope or container) for the classified documents. Place the wrapped documents in the pouch or briefcase (which serves as the outer container), and have the researcher secure the lock. If the researcher does not have a lockable container, NARA staff prepares both the inner and outer containers, ensuring that the documents are double-wrapped. The researcher must sign for the package contents on NA Form 2011, Classified Document Control Record, or other NARA-produced receipt, in accordance with Chapter 5 of this handbook.

(2) If a researcher needs copies of classified documents, but does not have a courier badge or memo, the documents are left with the classified research room monitor for later transmission to the researcher's agency. The monitor asks for a valid mailing address approved for the receipt of classified information at the classification level of the documents. Once the address is provided, NARA staff wraps and dispatches the information, as appropriate, in accordance with Chapter 5 of this handbook.

3.10 Prevention of Unauthorized Removal of Classified Records

While providing access to classified information is important, NARA must also protect these valuable and highly sensitive records from unauthorized removal, damage or destruction, including access to records provided electronically. In accordance with 44 U.S.C. 2108 note, the following procedures apply to research rooms and all NARA facilities authorized for the handling and storage of classified records. Cleared NARA staff responsible for providing access will ensure that:

a. no person, other than covered personnel (as defined in subpar 3.10f), will view classified records in any room that is not secure, except in the presence of cleared NARA staff (see par. 3.9c(8)) for when additional monitoring, to include video surveillance, may be appropriate);

b. no person, other than covered personnel, will at any time be left alone with classified records;

c. no person, including covered personnel, will conduct any review of classified records while in the possession of any cell phone or other portable electronic device prohibited under par. 4.13 of this handbook;

d. all persons seeking access to review classified records must, as a precondition to such access, consent to a search of their belongings upon conclusion of their records review; and

e. all notes and other writings prepared by persons, other than covered personnel, during the course of a review of classified records will be retained by NARA in a secure facility until such notes and other writings are determined to be unclassified, are declassified, or are appropriately transferred to another secure facility.

f.The term "covered personnel" (see also the glossary) means any individual who:

(1) has an appropriate and necessary reason for accessing classified records, as determined by the Archivist; and

(2) is either:

(a) an officer or employee of the United States Government with appropriate security clearances; or

(b) a Federal contractor with appropriate security clearances who has been authorized in writing to act for purposes of this section by an officer or employee of the United States Government.

3.11 Researcher Handling of Classified Information

a. If a NARA staff member suspects that a researcher is handling classified information inappropriately in the classified research room, he or she must:

(1) immediately contact the Secure Facility Manager (SFM), if applicable, or the cognizant ISPM. Notify the senior NARA official responsible for the research room, who will determine the initial course of action in consultation with the SFM, ISPM, Holdings Protection Team (HPT) and the NARA ISO; and

(2) request that a security officer respond and stand by to assist, as directed by the senior NARA official.

b. If a NARA staff member suspects that a researcher is taking classified information from the research room, politely ask the researcher to stay in the room and speak with the senior NARA official responsible for the research room. If the researcher refuses, or does not respond:

(1) activate the research room duress alarm, if available;

(2) request that a security officer respond, or call the local law enforcement emergency number (e.g., 911) for assistance;

(3) immediately notify the SFM, or alternate, and the senior NARA official responsible for the research room, who must promptly report the incident (or suspected incident) to the ISPM and the ISO.

(4) provide details as requested by security or law enforcement; and

(5) be prepared to identify and provide a full description of the researcher, the classification level and an unclassified account of the materials that you suspect to be missing.

c. Anytime there is evidence that a security incident may have occurred, follow the procedures in Chapter 9 of this handbook for reporting security incidents.

3.12 Interagency Agreement on Access for Official Agency Historians

Several agencies of the executive branch reached an interagency agreement effective on September 23, 1982, that allows official historians from other agencies signatory to the agreement to have access to each other's records as outlined in the agreement, reproduced here for convenience. Other statutory requirements governing the records may apply.

a. Text of Agreement. To facilitate the official governmental historical research projects, and in accordance with the provisions of Executive Order 11652 and its implementing National Security Council directive, the undersigned agencies agree to reciprocal rights of access, including the acquisition of copies, to classified materials now a part of accessioned Federal records or donated historical materials in the custody of the National Archives and Records Administration, provided that:

(1) access is limited to historians and historical researchers who are regular employees* of signatory agencies and are engaged in official research projects;

(2) access is limited to materials relevant to the researcher's official project and classified at or below the level of the researcher's clearances (access to Restricted Data limited to those with appropriate clearances); and

(3) materials and information derived from such access cannot be declassified or published without the consent of the agency of origin and must not otherwise be compromised.

* This agreement does not cover contract historians. Contract historians must make separate arrangements for access to classified materials; otherwise, they are treated as members of the public.

b. Addendum to the Agreement. In addition, and in accordance with the conditions stated in subpars 3.11a(1) through 3.11a(3) inclusive, the undersigned agencies agree to reciprocal rights of access, including the acquisition of copies, to classified materials more than ten years old now in the custody of the agency.

c. List of Signatories. The Central Intelligence Agency (CIA), Joint Chiefs of Staff (JCS) and National Security Council (NSC) did not sign this agreement. See subpar 3.11e for procedures regarding these agencies.

Agency	Main Body of Agreement	Addendum
Air Force	X	X
Army	X	X
Defense Intelligence Agency	X	NO
Energy	X	X
General Services Administration	X	X
Marine Corps	X	X
National Aeronautics & Space Administration	X	X
National Archives & Records Service	X	X
National Defense University	X	X
National Security Agency	X	X
Navy	X	X
Nuclear Regulatory Commission	X	X
Office of the Secretary of Defense	X	X
State	X	X

d. Instructions For Implementing The Agreement (from the Archivist's memo of February 24, 1978):

(1) The main text covers classified materials originated by a signatory agency and now in archival custody; to gain access, a signatory agency must certify to NARA that the person seeking access is an official agency historian (regular employee) on official agency business with clearances equal to that of the materials sought. Given those assurances, and barring any other barrier to access such as donor restriction or a privacy interest, the official historian may be permitted access. Copies of classified documents may be provided to the official historian. As a signatory of the agreement, NARA authorizes access to materials classified by the President or the White House staff of an Administration (excluding materials classified by the National Security Council staff). The addendum of the agreement covers classified materials still in the agency of origin; for NARA this means classified materials in the custody of NARA that are not accessioned records. Access to these materials may be gained by presentation of a letter containing the elements described above, but NARA forwards a copy of such letter to the classifying agency for the information of the agency.

(2) Because not all agencies are signatories of the Agreement, archivists have to review requested files and remove classified documents originated by non-signatories before providing access to the files. Official historians should be informed that they must seek permission from any non-signatory agency, other than the CIA or JCS [(sic) and NSC], in order to obtain access to classified materials originated by the non-signatory.

e. Procedures for CIA, JCS and NSC:

(1) CIA. In a letter, dated 30 January 1978, to Dr. James E. O'Neill from Dr. Jack B. Pfeiffer, CIA historian, the CIA extended its "Revised (12 July 1977) Access Policy Concerning Presidential Libraries" to all CIA originated materials in the custody of the National Archives and Records Administration. This policy is as follows:

(a) Direct incoming requests from other agencies to the CIA Historian for initial review. The requesting agency must identify its responsible historian by full name and rank (if military) and by type of employment (staff, contract, or other), and must certify the researcher's level of security clearance.

(b) A brief statement of proposed research requiring access to CIA documents accompanies the initial request and establishes the "need to know". The CIA historian approves or denies the research request ---consulting, if needed, with the CIA components most directly concerned.

(c) Once a project is approved, the CIA Historian notifies the requesting agency, NARA, and the specified Presidential library. An official historian using a Presidential library is free to take notes and to have the library make copies of the documents to be retained for research purposes.

(d) Staff at the Presidential library collect all such notes and copies of CIA documents desired by requesters and forward them to the CIA Historian for review before release. The CIA Historian asks the originating CIA components to review requested documents or notes requested by other agency historians, and transmits the items (or notes their denial) to the requester.

(e) As in the past, if a requesting agency contemplates overt publication of a given history, formal security review and clearance procedures require agency concurrence on the inclusion of information based on Agency originated documents.

(2) JCS. In a letter dated December 14, 1977, Arion N. Pattakos, Secretary of the Joint Chiefs of Staff, stated that "the policy of the Joint Chiefs of Staff precludes carte-blanche access to JCS records by outside agencies until the records have been reviewed and declassified". If an agency historian seeks access to classified JCS documents, NARA forwards copies of the requested records to the JCS for declassification review. Contact the NARA ISO to verify the current address:

Chief, WHS Declassification Branch
ATTN: [Incumbent]
Washington Headquarters Services
1155 Defense Pentagon

Washington, DC 20301-1155

(3) NSC. All NSC-originated materials or other documents containing NSC equities in the custody of the National Archives and Records Administration may be provided to other agency historians who possess the appropriate clearance, if approved in writing by NSC on a case-by-case basis. NARA refers NSC, White House, and NSC-interest records to other agencies for review when appropriate.

3.13 Controlled Access Information

Access to the following additional categories of classified information with security measures exceeding those normally required for information at the same classification level is more stringent than the general requirements in par. 3.1.

a. RD/FRD Access Requirements. Initial access authority to RD/FRD information must be adjudicated at DOE in accordance with the Atomic Energy Act of 1954, as amended, and is only granted to those individuals who have a need to know and already have the appropriate security clearance. BX maintains a list of all individuals at NARA who have been granted access. RD/FRD information in the possession of NARA must not be turned over to any contractor or subcontractor engaged by NARA unless he or she holds one of the following access levels granted by DOE:

(1) "Q" access indicates that an individual is approved for access to both RD and FRD information at the Top Secret, Secret, and Confidential levels on a need to know basis; or

(2) "L" access indicates that an individual is approved for access RD information at only the Confidential level, and to FRD information at only the Secret and Confidential levels, on a need to know basis.

b. SCI Access Requirements. Access to SCI must be adjudicated at CIA and is only granted to those individuals who have a need to know and require access to SCI to perform their job. NARA supervisors request access for their personnel by sending a memo, with justification, to BX, to prepare and forward a nomination package to CIA. Nominated individuals must be eligible for Top Secret security clearance, and successfully undergo a Single Scope Background Investigation (SSBI) that shows they meet the personnel security standards of ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information. The SSBI are updated every 5 years for as long as the individual requires access. The CIA bases the approval on review of the nomination package and the SSBI. Once granted access, individuals are given an indoctrination briefing by BX or other designated personnel. BX maintains a list of all individuals at NARA who have been granted SCI access.

c. SAP Access Requirements. When SAP information is delivered to NARA, the owning agency must provide required handling procedures (usually in the form of a Security Classification Guide) and a list of authorized individuals who may continue to need access to the information. Access to SAP information requires a final security clearance at the

classification level of the program to which access is sought. All NARA personnel requiring access to SAP information must be vetted by the owning agency's Program Security Officer (PSO) and added to the PSO's access list. PSOs maintain separate access lists for each SAP. SAP information cannot be accessed by persons from either NARA or the owning agency unless their names are on the access list for that program. Verify or request access by contacting the appropriate PSO.

d. NATO Access Requirements. Access to NATO classified information requires a final U.S. security clearance at the equivalent classification level (i.e., access to NATO COSMIC Top Secret requires a U.S. Top Secret security clearance and access to NATO Secret information requires a U.S. Secret security clearance). Access to NATO classified information must be limited to the minimum number of personnel who require access to do their assigned duties. NARA sub-registry control officers conduct briefs and debriefs of all NARA employees who require NATO access, maintain a list of those granted access, and provide copies to the NARA Personnel Security Officer for inclusion in the agency personnel security file.

3.14 Access Briefing and Debriefing Forms

The following forms are used during initial briefings and termination briefings to officially document an individual's access to the various categories of classified information:

a. Standard Form (SF) 312, Classified Information Nondisclosure Agreement. The SF 312 is required to be signed by every individual before access is granted access to classified information. The form must be signed and provided to the Personnel Security Officer within 15 workdays after an individual occupies a sensitive position requiring a security clearance; otherwise, the clearance may be voided. The back portion, Security Debriefing Acknowledgement, is used when debriefing individuals who no longer need access to classified information. See Chapter 8, par. 8.4 for additional information.

b. Form 4414, Sensitive Compartmented Information Nondisclosure Agreement. Form 4414 is required to be signed by every individual before access is granted to Sensitive Compartmented Information (SCI). The back portion, Security Briefing/Debriefing Acknowledgment, is used when debriefing individuals who no longer need access to SCI.

c. SAP Format 2, Special Access Program Indoctrination Agreement. This form may be used only by the originating agency's PSO to grant SAP access to an individual, after the access has been formally requested and approved using SAP Format 1, Program Access Request.

d. DOE F 5631.18, Department of Energy Security Acknowledgement. DOE F 5631.18 must be signed by every individual who is granted access to Restricted Data (RD) and Formerly Restricted Data (FRD).

e. DOE F 5631.29, Department of Energy Security Termination Statement. DOE F 5631.29 is used when debriefing individuals who no longer need access to RD and FRD information.

f.NATO Briefing/Debriefing Certificate must be signed by every individual at NARA who is granted access to NATO classified information. Section D, at the bottom of the form, is used when debriefing individuals who no longer need access.

NOTE: All briefing and debriefing forms, except for SAP Formats 1 and 2, must be sent to BX upon completion. Individuals requesting access will forward original SAP briefing and debriefing forms to the originating agency's PSO.

[Return to TOC]

Chapter 4

SAFEGUARDING

4.1 General

Classified information may be used, held, or stored only where facilities and conditions are sufficient to reasonably prevent unauthorized persons from gaining access to it. The requirements in this handbook represent the minimum acceptable standards.

4.2 Receipt and Handling

Responsibility for safeguarding classified information begins when it is received at NARA or created at NARA through other means, such as copying documents or portions thereof for facilitating research or reviews. Maintain security of the information until it is destroyed, declassified, or otherwise disposed of.

a. Records transferred to the physical custody of a NARA records center are documented on SF 135, Records Transmittal and Receipt, or an electronic equivalent. The presence of classified information must be noted on the form.

b. Records transferred to the legal custody of the National Archives of the United States from an agency of the Federal Government are documented on an Electronic Records Archives (ERA) Transfer Record (TR). The presence of classified information, and the level of classification, is indicated on the TR.

c. Presidential and White House-originated records and donated historical materials may be accompanied by a variety of documentation, such as a box list, inventory, or similar documents. The transferring documents must indicate the presence of classified information, the level of classification, and any special handling instructions.

d. When classified information is received at a NARA facility, it must be delivered to cleared personnel designated to receive it with the inner container unopened. If there is any doubt as to the intended recipient, contact the cognizant ISPM.

e. The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained and reported promptly to the cognizant ISPM, who immediately notifies the ISO under the reporting guidelines of Chapter 9. Discrepancies in the contents of a package must be reported immediately to the sender. If the shipment is in order and includes a receipt, the receipt must be signed and returned to the sender. Maintain a copy of the signed receipt in the files of the receiving office. Refer questions to your ISPM.

f.If no documentation accompanies transferred records, request it immediately from the transferring entity or its successor, as appropriate. Treat material received without

accompanying documentation that reasonably could contain classified information as classified until it is determined otherwise.

g. Route the notification of receipt or, if possible, a copy of the form (SF 135 or SF 258) or box list to the cognizant ISPM who makes sure the records are protected until a decision is made on the level of classified information and whether it is subject to access or other controls.

h. Offices must develop local procedures to ensure all incoming U.S. mail, parcel and courier deliveries are properly protected as classified until they are determined to be otherwise. Establish screening points to ensure that incoming material identified as, or determined to be classified is properly controlled and that access is limited to cleared personnel.

i. Use NA Form 2011, Classified Document Control Record, as explained in pars. 5.4 and 5.5, or other equivalent NARA-produced document receipt, for any classified information dispatched outside NARA facilities.

4.3 Administrative Management

a. Maintain an automated database, or other suitable control system for classified information held at NARA archival facilities, records centers and Presidential libraries that is received or generated. This may consist of one or multiple data sources, which, at a minimum, allows identification of records sufficient to investigate loss or compromise. The record must include any controlled category (e.g., NATO, RD/FRD, SCI, etc.), receipt data, and information on internal distribution or status, referral to equity holders, and final disposition or destruction. Specific examples of systems suitable for control and identification of classified information include, but are not limited to, the NARS-5, 01 Report and the Archives and Records Centers Information System (ARCIS) used at records centers, the Accessions Management & Information System (AMIS), the Archival Preservation System (APS), the Archives Declassification, Review and Redaction System (ADRRES), the Remote Archives Capture (RAC) Project, and any NARA-approved withdrawal card (currently those in the 14000 series).

b. Maintain documentation for individual records only when mandated by the governing directive for special categories of classified information as referenced in par. 4.4, or by special agreement with the transferring agency. Otherwise, safeguard documents at the folder or box level for textual documents, and at the media volume level for electronic records, in accordance with the provisions of this handbook. ISPMs ensure that offices maintain records of external receipt and dispatch sufficient to investigate loss or compromises of classified documents during transmittal.

c. Records in NARA's Physical, but Not Legal, Custody:

(1) Agency-controlled records containing classified information that are transferred to a records center facility are controlled in accordance with any special agreement with the transferring entity. In the absence of an

agreement, the provisions of this handbook and Records Center Operations Manual (NAR P 1864.1A) apply.

(2) Presidential records containing classified information that are in courtesy storage are controlled by special written agreements between the Office of Presidential Libraries and the White House. Without such agreements, the provisions of this handbook apply to NARA's handling of the records.

(3) Congressional records (those of the U.S. House of Representatives and the U.S. Senate) in NARA's physical custody are subject to the rules of their respective chamber (44 U.S.C. 2118). Under these rules, the Office of the Clerk of the House and the Office of Senate Security, on behalf of the originating committee, can request the loan of original classified records in NARA's physical custody for use by the committee that created the documents. NARA provides courtesy storage under memoranda of agreement between NARA and the originating committees.

(4) Agency-controlled electronic records containing classified information that are transferred to the National Archives for appraisal and accessioning must be registered upon receipt in appropriate administrative management systems, that identify and locate media volumes.

d. Records in NARA's Legal Custody. Records containing classified information accessioned or legally transferred into the National Archives of the United States are controlled under the provisions of 36 CFR Part 1256, and subpar 3.5b of this handbook.

e. Loans. Original, accessioned classified records normally are not loaned for declassification review or for research outside of a NARA facility. Exceptions may be made by the Archivist under agreement with the originating or reviewing agency.

f.Telephone Conversations. Classified information must be discussed on an approved device, such as Secure Telephone Equipment (STE), and never on a standard office desk (unclassified) telephone.

g. Security of Large Meetings or Conferences. Following the guidance in par. 4.11, coordinate security requirements for large meetings or conferences, at which classified information is discussed or disclosed, with your ISPM or the NARA ISO.

4.4 Safeguarding Controlled Access and Foreign Government Information

Control and safeguarding of Restricted Data/Formerly Restricted Data (RD/FRD), Sensitive Compartmented Information (SCI), Special Access Program (SAP), NATO, COMSEC, FGI, and any required documentation, must be compliant with applicable provisions of this handbook and the following respective governing regulations:

a. Control and safeguard RD/FRD in accordance with DOE Order 471.6, Information Security, and 10 CFR Part 1045, Nuclear Classification and Declassification.

b. Control and safeguard SCI in accordance with ICD 703, Protection of Classified National Intelligence Including Sensitive Compartmented Information; ICD 705, Sensitive Compartmented Information Facilities; and ICD 503, Information Technology Systems Security Risk Management, Certification and Accreditation.

c. Control and safeguard SAP information in accordance with the governing directives of the SAP originator, 10 U.S.C. 119, 50 U.S.C. 2426, this handbook, and the National Industrial Security Program Operating Manual (NISPOM), as applicable.

(1) If SAP information appears in records in NARA's legal custody, it belongs to NARA and must be protected in accordance with the documentation provided at the time the material was turned over to NARA. If SAP information is in records not in NARA's legal custody, complete a Memorandum of Understanding (MOU) between the owning agency and NARA. This serves as a "contract" between the two agencies to define each agency's roles and responsibilities for safeguarding and controlling the SAP information.

(2) Additionally, the cognizant security authority for the secure facility in which the SAP information is to be stored must agree to have SAP information stored within their facility. Execution of a Co-utilization Agreement (CUA) satisfies this need. The CUA formally authorizes the facility to be "co-utilized" for storage of SAP information and other forms of classified information, including SCI. It details how the information is to be stored, controlled and segregated from all other classified information stored in the facility. SAP information must not be introduced into any secure facility without first obtaining a completed CUA. The SFM, or cognizant ISPM, contacts the NARA ISO to obtain a CUA. Copies of all authorizing documentation must be maintained in the secure facility management folder within the secured area.

d. Control and safeguard NATO information in accordance with United States Security Authority for NATO Affairs (USSAN) Instruction 1-07, Implementation of NATO Security Requirements. NATO has established central points of control for NATO information within each NATO member nation. The control point for the United States is the Central U.S. Registry (CUSR) located at the Pentagon.

(1) The CUSR has recognized five NATO subregistries and one control point within NARA for managing classified NATO information that is being stored or accessioned from other executive branch agencies:

(a) National Declassification Center (ANDC);

(b) George H. W. Bush Presidential Library (LP-GB);

(c) William J. Clinton Presidential Library (LP-WJC);

(d) Ronald Reagan Presidential Library (LP-RR);

(e) George W. Bush Presidential Library (LP-GWB); and

(f) Dwight D. Eisenhower Presidential Library (LP-DDE) (NATO control point).

(2) Each NATO subregistry and control point in NARA must appoint a NATO Document Control Officer, and one or more alternates as necessary, to implement standard procedures for protection of NATO information and limit distribution and access to only those who need to know and have the appropriate security clearance. All appointed individuals must also be listed on a DAAG Form 29, Subregistry/Control Point Signature List, which each person must sign. Subregistries send the original DAAG Form 29 to the CUSR; control points send the DAAG Form 29 to the National Declassification Center. Maintain a copy of USSAN 1-07 on site and refer to the CUSR web site for additional guidance (look under "Security References" on the Safety, Security & Emergency page of the NARA@work web site).

(3) Submit one copy of all appointment letters, the completed DAAG Form 29, and briefing/debriefing certificates to BX. Report any changes in the designation of control officers as they occur. BX provides NARA subregistries with up-to-date computer print-outs of their NATO-accessed personnel, as requested.

(4) Procedures. NATO Document Control Officers at NARA:

(a) route all NATO classified documents internally or to external agencies only through other designated NATO subregistries or control points, except as permitted in subpar 4.4d(5) below;

(b) conduct initial briefing and debriefing of NARA personnel requiring access to NATO classified information;

(c) conduct annual security awareness briefings for all NARA personnel to whom they have granted access to NATO classified information;

(d) accomplish annual inventories of all classified NATO documents on file or loaned, consistent with the provisions of par. 4.3 in this handbook, and submit the results to the CUSR when requested, usually during the first quarter of the calendar year (maintained under item 261-3c of the NARA records schedule); and

(e) perform self-inspections every 24 months as required by USSAN 1-07.

(5) NATO Document Control Officers may release COSMIC and ATOMAL documents outside a subregistry or control point only on a temporary loan basis to individuals who are cleared, responsible for their custody, and can

provide adequate storage facilities. COSMIC and ATOMAL documents must be returned to the NARA subregistry from which they were loaned when no longer needed. Control officers must maintain a record of the location of documents on loan.

(6) Superseded NATO documents and those no longer needed for agency business that are in NARA's physical, but not legal custody may be reviewed by the equity holding agency and managed in accordance with the applicable NARA-approved records schedule.

e. Control and safeguard COMSEC information and material in accordance with the National Security Agency/Central Security Service (NSA/CSS) Policy Manual 3-16, Control of Communications Security (COMSEC) Material, Committee on National Security Systems Instruction (CNSSI) 4001, Controlled Cryptographic Items, and CNSSI-4005, Safeguarding COMSEC Facilities and Materials. BX appoints a COMSEC Control Officer and alternate for management and control of all COMSEC-related equipment and controlled information at NARA. NARA personnel must coordinate with the COMSEC Control Officer on all associated matters, or for any type of necessary COMSEC equipment. Secure telephone equipment (STE) is the most common form of COMSEC equipment familiar to NARA personnel.

f.Control and safeguard FGI in accordance with existing treaties or agreements and 32 CFR Part 2001.54.

(1) Top Secret level FGI must have records of receipt, dispatch, internal distribution, and access. Reproduction for anything other than routine declassification review requires the consent of the originating government.

(2) Secret level FGI must have records of receipt and dispatch. It may be reproduced to meet NARA requirements unless specifically prohibited by the originating government.

(3) Confidential level FGI does not require documentation unless the originating government requires it.

(4) Restricted level FGI is a fourth category that does not correspond to an equivalent U.S. classification level, but is used by some foreign governments. Safeguard Restricted FGI in the same manner as U.S. Confidential information.

(5) Some FGI is provided to the United States on the condition that it is protected "In Confidence." Documents in this category are not classified, but must be protected from public release and handled in accordance with 32 CFR Part 2001.54(d).

4.5 Industrial Security

a. E. O. 12829, as amended, National Industrial Security Program (NISP), establishes and provides guidance for the safeguarding of classified information that is released to contractors, licensees and grantees of the U.S. Government.

(1) The ISOO implementing directive, 32 CFR Part 2004, National Industrial Security Program Directive No. 1, provides required policy direction for all executive branch departments and agencies. The NISP establishes the Secretary of Defense as the executive agent for oversight of the industrial security program for executive agencies.

(2) 32 CFR Part 117, National Industrial Security Program, and the National Industrial Security Program Operating Manual (NISPOM), both promulgated by DoD for implementing E.O. 12829, as amended, prescribe specific requirements, restrictions, and other safeguards that are necessary to control classified information and preclude unauthorized disclosure during all phases of the contracting process. The NISPOM also prescribes requirements, restrictions and other safeguards that are necessary to protect special classes of classified information, including RD, FRD, intelligence sources and methods information, SCI, and SAP information that are handled by government contractors.

b. Before issuing or soliciting bids on a contract that requires industry to have access to classified information at the contractor's facility, coordinate with the NARA ISO to verify that the prospective contractor has a facility security clearance and appropriate storage facilities.

c. Use the sample DD Form 254, Contract Security Classification Specification, and the Contractor Security Agreement (CSA) as templates to establish the requirements for industry when performing work under classified contracts with NARA. The DD Form 254 and CSA may need to be adjusted, based on the particulars of each contract, and contractors must comply with the stipulations set forth in the CSA and the DD Form 254. All contracts issued by NARA that involve classified information must include a CSA with a DD Form 254 that is certified and signed by the NARA ISO. Further guidance is available on the Safety, Security & Emergency page of the NARA@work web site.

d. Regardless of the performer of the work, contractors with this CSA incorporated into their contracts are responsible for compliance with the requirements of the CSA. Affected contractors are also responsible for imposing the requirements of the CSA to subcontracts at any tier to the extent necessary to ensure the subcontractors' compliance with the requirements. In so doing, contractors must not unnecessarily or imprudently impose requirements to subcontractors. That is, contractors ensure that they and their subcontractors comply with the requirements of the CSA and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

e. A violation of the provisions of the CSA relating to the safeguarding or security of classified information may constitute a violation of United States criminal laws under the provisions of 18 U.S.C. 641, 793, 794, 798, and 1924.

f.The complete CSA is comprised of the DD Form 254, the signed agreement, and NARA 202.

4.6 Reproduction

a. Only make copies of documents containing classified information as necessary.

b. Copies of classified documents must have the same classification markings as the original document.

c. Control copies with the same controls as the original document.

d. Do not reproduce classified information that prescribes a restriction against its reproduction without the authorization of the originating agency, except for the purpose of referral for declassification review or to respond to a statutory special access review. Document the authorization and the number of copies made by a notation on the copied material.

e. Only cleared persons knowledgeable of the procedures for classified reproduction may copy classified information.

f.Classified information may not be reproduced in the presence of uncleared individuals.

g. Copying Equipment:

(1) Classified documents may be reproduced only on equipment that has been approved for that purpose by the ISO or cognizant ISPM. NA Form 2007, Equipment Authorized for Reproduction of Classified Material, must be conspicuously posted on or near the machine. All machines used for classified reproduction should incorporate as many security design features as possible, e.g., pass code lock, copy counter, removable hard drives, encryption of data prior to being stored in memory and on hard drive, and data overwrite (all memory automatically cleared after copy). You should also avoid or mitigate certain technologies, for example:

(a) machines designed with remote diagnostic capabilities are not authorized in classified environments;

(b) if a computerized diagnostic device (such as a laptop) is used to perform on-site maintenance or troubleshooting on machines, a compatible diagnostic device should be purchased along with the reproduction equipment to ensure maintenance capability for machines located in secure facilities;

(c) digital copiers used for classified reproduction will be used only in a stand-alone capacity (not connected to any network or telephone line); and

(d) machines authorized for classified reproduction that are located outside of secure facilities must not have hard drives or the capacity to retain memory or images. See the Safety, Security & Emergency page of the NARA@work web site for more information on copier security and related concerns with reproduction equipment.

(2) Classified reproduction equipment must either be located in a secure facility or access must be restricted while copying is in progress, and the equipment and surrounding area must be thoroughly sanitized when finished. SCI information may only be copied in a SCIF.

(3) Users of classified reproduction equipment should check it periodically to ensure the equipment is not retaining a latent image. If a blank sheet of paper passed through the machine shows an image or shadows when no document is on the platen, the machine is malfunctioning and must be repaired. Any pages with a latent image must be protected or destroyed in an approved manner. Equipment that leaves latent images either on the equipment, original documents, or reproduced copies is prohibited for SCI reproduction. ISPMs must recertify classified reproduction equipment during self inspections to make sure they are working properly and annotate the NA Form 2007 accordingly.

4) NA Form 2021, Classified Reproduction Prohibited, must be conspicuously posted on or near equipment used only for the reproduction of unclassified information, except for those in public access areas.

(5) Classified reproduction equipment may not be removed from NARA facilities without inspection by the cognizant ISPM.

4.7 Storage

When classified information is not under the physical control and observation of an authorized person, store it as follows:

a. Top Secret information must be stored in:

(1) a General Services Administration (GSA)-approved security container with a built-in, three-position dial-type changeable combination lock, within a building or room that is locked and guarded or protected by an alarm system during non-duty hours;

(2) an alarm-protected secure facility, determined by the NARA ISO to afford protection equal to or better than that prescribed in the preceding paragraph; or

(3) an alarmed area approved by the NARA ISO, with a physical barrier adequate to prevent surreptitious removal of the information or observation

that shows evidence of attempted forced entry. The alarm system must provide immediate notice to the security force of attempted entry.

b. Secret information must be stored in:

(1) the same manner authorized for Top Secret; or

(2) a GSA-approved security container within a locked room.

c. Confidential information must be stored in:

(1) the same manner authorized for Top Secret and Secret information; or

(2) a GSA-approved security container.

d. Classified Information Subject to Access Controls. Sensitive Compartmented Information (SCI) must be stored only in an SCI facility (SCIF) that has been constructed and approved by the cognizant security authority in accordance with ICD 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities. Information subject to other access controls, such as Restricted Data/Formerly Restricted Data (RD/FRD) and Special Access Program (SAP) information, must be segregated and stored according to DOE Order 471.6, Information Security, governing directives of the SAP originator, this handbook, and any other procedures prescribed by the responsible agencies or departments.

e. Use of Federal Records Center (FRC) "Hand Hole" Cartons for Storage of Classified Information. FRC boxes with "hand holes" meet the standards to store classified information, inside an approved storage facility or container, with a slight modification to the packing procedure. For those boxes containing classified information, blank opaque file folders must be placed inside the box, at both ends, so that the contents are not visible to unauthorized persons.

f.Storing Cash and Valuables. Money, jewelry, weapons, or articles of high intrinsic value must not be stored in the same container with classified information.

4.8 Construction Requirements for Secure Facilities

a. The physical construction requirements for open storage of classified information up to the Top Secret level are contained in 32 CFR Part 2001.53 (and the NISPOM, sections 5-801 and 5-802, as applicable). This guidance specifies the minimum safeguards and standards required for the approved storage of classified information.

b. Physical construction requirements for a SCIF are contained in ICD 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities. Construction requirements differ slightly dependant on whether the SCIF is located in the U.S., and authorized for closed or open storage. The referenced guidance specifies the minimum standards required for the construction of SCIFs approved for use as handling or storage facilities for SCI material.

c. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. Also, they may be used for evaluating the adequacy of those areas.

4.9 Security Containers and Locks

Security containers used for the protection of classified information must be GSA-approved equipment identified on the GSA Federal Supply Schedule's approved list of security containers. Locks that protect classified information must meet the requirements of Federal Specification FF-L-2740.

a. Available Types or Classes of Containers. Class 6 containers are GSA-approved for the storage of Secret, Top Secret, and Confidential information. Protection for 30 man-minutes against covert entry and 20 man-hours against surreptitious entry. No forced entry requirement. Class 5 containers are GSA-approved primarily for the storage of weapons, narcotics and controlled substances, or other high-value materials; however, they can also be used for storage of classified information. Protection for 30 man-minutes against covert entry and 10 man-minutes against forced entry, and 20 man-hours against surreptitious entry. Class 6 and Class 5 security containers are sized to accommodate either legal or letter size materials; please select the appropriate size when ordering.

b. Designated Custodian. The ISPM, SFM, or other appropriately cleared individual(s) so designated by the using office assumes custodial responsibility for all security containers located within their assigned spaces. Post an SF 702, Security Container Check Sheet, on the security container. Individual(s) opening or closing the container must annotate the SF 702 with their initials, date and time. Security containers with individually locking drawers require an SF 702 for each drawer. Maintain completed check sheets in operational files for at least 3 months following the last entry on the form, in accordance with NARA records schedule, item 259-2. Also, custodians and authorized users of classified information must:

(1) implement the policies and procedures of this handbook to prevent, deter, and detect unauthorized access to classified matter stored in assigned security container(s);

(2) ensure that classified information is properly secured when not in use or under the direct supervision of authorized persons;

(3) ensure that security containers are located within rooms or buildings that provide supplemental protective measures, when required, in accordance with par. 4.7 of this handbook; and

(4) adhere to the requirements of subpars 4.9b through 4.9e, inclusive.

c. Numbering Security Containers. Each container used for storing classified information must be primarily identified by the manufacturer's serial number embossed on a small metal plate affixed at the top front of the container. Do not remove this metal plate. When an office is responsible for more than one security container, they may be numbered and

labeled sequentially for administrative convenience and control; however, maintain a cross-reference to the manufacturer's serial number for identification purposes. Do not mark or label security containers on the outside showing the level of classified information stored within them.

d. Protection of Combinations, Access Codes and Personal Identification Numbers (PINs). Only authorized persons may have knowledge of combinations, codes and PINs to authorized security containers, and secure facilities.

(1) Record the names of persons having knowledge of the combination, who must be contacted if the security container is found open and unattended, on SF 700, Security Container Information. Attach Part 1 of this form inside the locking drawer of each security container, or the interior side of the primary secure facility door. Record the combination number(s) on Part 2A of the form, insert it into the attached envelope (Part 2), and seal the envelope.

(2) Mark and safeguard the SF 700 envelope containing the combinations at the highest classification of the information authorized for storage within the container or facility. Maintain the SF 700 under item 259-1 of the NARA Records Schedule and destroy superseded combinations in accordance with the guidance in Chapter 7 of this handbook. ISPMs must maintain the sealed SF 700 envelopes, for security containers and facilities under their cognizance, within a separate container or facility of equal or higher accreditation/classification level. Records of these security combinations and the names of individuals who know them, as reflected on the SF 700, are considered vital records according to Federal continuity directives; therefore, the responsible ISPM or SFM must know where they are maintained and make them available for quick reference and access when necessary in an emergency.

(3) Combinations to the GSA-approved security locks may only be shared with a minimum number of people (normally two to four) who must be clearly identified on the SF-700 or other listing provided to BX. Do not provide these combinations to anyone not thus identified. Limit access to records and information concerning other codes and PINs for secure facilities to personnel on that facility's access roster. Individuals given such information must not share it with any other individual. The SFM is the primary administrator of the Intrusion Detection System (IDS) and must change combinations and remove access codes and PINs from the system whenever a person with access is transferred, terminated, or when their access is suspended, revoked, or downgraded to a level below that required for entry. Immediately report any compromised combinations, codes or PINs to the SFM and to the NARA ISO. In accordance with NARA 202, subpar 202.4e(2), the ISO reports such compromises to the OIG when a violation of criminal statutes is suspected.

(4) Do not write down combinations, passwords, PIN numbers, and the like, to carry with you as reminders. Such information could allow unauthorized individuals to gain access to classified information and carrying combinations in your purse or wallet, for example, is a practice dangerous to security that risks compromise of the information NARA must protect.

(5) The cognizant ISPM, SFM, designated custodian, or other appropriately cleared individual sets and changes security container combinations. Combinations must be changed when:

(a) a container is first used after procurement;

(b) a person who knows the combination is transferred, discharged, or reassigned from the unit that holds the container, or when the security clearance of a person who knows the combination of it is reduced, suspended, or revoked by proper authority;

(c) the combination or a record of the combination is compromised or when the security container is found unlocked and unattended (report such incidents in accordance with Chapter 9 of this handbook);

(d) maintenance work on the container is done by persons other than the custodian;

(e) NATO information is stored in a container and the combination has not been changed for any other reason in the previous 12 months; or

(f) a container is taken out of service (built-in combination locks must be reset to 50-25-50; combination padlocks must be reset to 10-20-30).

e. Cipher and Electrically Activated Locks. Cipher and electrically activated locks (e.g., cipher locks and magnetic strip cards) do not provide enough protection by themselves for secure facilities and may not be substituted for the locks prescribed in par. 4.9; however, they may be used as supplemental protection for secure facilities to admit or deny entry to an occupied area, provided:

(1) the lock is properly installed and used in a manner to prevent unauthorized viewing;

(2) the combination is changed by an authorized person whenever any of the conditions listed in subpar 4.9c(5)(a) through (f) exist; and

(3) the combination is protected according to subpar 4.9d.

f.Repair of damaged security containers or locks must be performed in accordance with Federal Standard 809A in consultation with BX.

4.10 Establishment and Operation of Secure Facilities

Secure facilities at NARA must be configured to meet the specifications of ICD 705, 32 CFR Part 2001 and this handbook, as applicable. They must be surveyed and accredited before using for storage, discussion, or processing of classified information by the appropriate cognizant security authority. At NARA, the cognizant security authority for secure facilities at the Top Secret level and below is BX. The CIA is the primary cognizant security authority for secure facilities at the SCI level, with BX being secondary. BX and CIA may, at any time, perform oversight inspections for the facilities over which they exercise cognizance. The following guidance may be used to form the basis of Standard Operating Procedures (SOP) required for any secure facility.

a. Establishment. In order to establish an accredited secure facility for the protection of classified information, a NARA office must:

(1) have a permanent or recurring need to store, discuss or process applicable classification levels and categories of classified information;

(2) coordinate with the NARA ISO to identify and survey the area to be configured as a secure facility;

(3) complete, or assist the ISO in completing, a Fixed Facility Checklist (FFC) to document the security posture of the proposed facility;

(4) work with the ISO to develop a Statement of Work (SOW), obtain necessary construction plans, schematics, pictures, etc., and after approval by the cognizant security authority, have the facility configured to required specifications; and

(5) notify the ISO before any subsequent renovation, modification, or other changes to the facility.

b. Operation. The NARA office responsible for the facility appoints a Secure Facility Manager and alternate (see NARA 202, subpars 202.4g, 4h and 5d) who:

(1) operate the secure facility and provide general and overall security management and security oversight for activities within the facility;

(2) develop an SOP for the secure facility and keep it updated (this SOP, including changes, must be submitted to the NARA ISO, through their ISPM, for review and approval before implementation);

(3) post NA Form 6051, Secure Area Notice, in a conspicuous location on or near the entrance door and performs access and visitor control functions within the secure facility in accordance with subpar 4.10c of this handbook;

(4) maintain a roster of individuals authorized access to the secure facility (who must be required to acknowledge, in writing, that they have read and understand the secure facility SOP and are familiar with the handling of classified information in accordance with NARA 202);

(5) create a six-part facility management folder to maintain accreditation documents and other record information within the secure facility, under items 262 and 263 of the NARA Records Schedule, consisting of (in the order shown):

(a) accreditation letters for the facility and any computer systems operating within the secure facility, plus any other pertinent documentation affecting the status of the facility, such as Memoranda of Agreement or Understanding (MOA/MOU) with other agencies regarding the use of SAP information or other documents containing their equities (first);

(b) completed FFC, as applicable, and any facility inspections (second);

(c) alarm test records to include initial and all subsequent tests (third);

(d) appointment letters for the SFM, and alternate (fourth);

(e) a facility access roster using NA 6068, Secure Facility Access Roster (fifth) (see par 4.10c(1)); and

(f) an approved SOP and Emergency Action Plan (EAP) according to subpar 4.10e (either combined or two separate documents) tailored specifically for the secure facility (sixth).

(6) provide the ISO with updated facility management folder documents, whenever a change occurs in any of the information;

(7) ensure secure facility occupants follow the secure facility's EAP and general building emergency procedures (NARA general emergency procedures are located on the NARA@work intranet site);

(8) as system administrators for the access control and alarm systems within the secure facility, assign and remove card access and PINs (where applicable) and follow the procedures in subpar 4.10c and par. 4.11 of this handbook to grant or deny access to the secure facility;

(9) test the alarm system, and security response where applicable, once every six months in accordance with subpar 4.10d of this handbook;

(10) attend annual and periodic information security education and training provided by their ISPM or the ISO, and conduct reciprocal annual and periodic training for staff members who regularly work within the secure facility; and

(11) conduct annual self-inspections to ensure compliance with the policies and procedures listed in this handbook (maintaining self-inspection results in the secure facility management folder, with a copy to their ISPM).

c. Personnel and Physical Access Controls:

(1) Secure Facility Access. The SFM develops an access roster using NA 6068, Secure Facility Access Roster, and keeps it current. Only appropriately cleared personnel under the control or sponsorship of the office responsible for the secure facility may be listed on the NA 6068. A printed and signed NA 6068 (all parts) must be submitted through the ISPM to the Information Security Officer. Maintain a copy of Part B of the access roster inside the facility at the entry point. Provide a copy of Part A of the access roster to the security control station responsible for monitoring the facility. At Archives I and II, BX will use the NA 6068 to update the access control database, then forward a copy of Part A to the Security Control Center (SCC).

(a) When only making changes to Parts B and C of the NA 6068, the updated pages may be sent electronically to the ISO.

(b) Anytime there are changes to Part A, or the date on the latest Part A is older than one year, the SFM must resubmit a complete, printed and signed NA 6068 through their ISPM.

(c) SFMs at locations where access is managed through a centrally controlled automated access control system (ACS) (e.g., Archives I and II) may use the "alternative" Part B of the NA 6068, since contractor/other agency VAL expiration dates can be tracked by the Security office in the ACS. Instead, the additional access column may be used to grant further access to such things as lockdown shelving ranges within the secure facility that are also controlled by the ACS.

NOTE: Security control will contact individuals listed on Part A of the access roster if the secure facility is found open and unattended after hours, or if there are any problems with the alarm system, including power failures.

(2) Occupancy. Prior to opening a secure facility, individuals must annotate the SF 702 posted on the entrance door with their initials and the date/time the facility was opened. Notify security before entering the facility and deactivating the IDS. Once the secure facility has been opened and the alarm deactivated, access must be controlled by either a NARA employee who has the appropriate clearances and SCI access, or by a two-factor access control system (e.g., badge and PIN reader). If the secure facility is a SCIF, an ACS shall not be used to secure it when unoccupied. When not occupied, SCIFs shall be alarmed and secured with an approved combination lock. If, for whatever reason, alternate arrangements for control of the secure facility during periods of occupancy or unoccupancy are necessary, obtain written approval from the accrediting authority through the ISO. Include any approved recurring procedures in the secure

facility's SOP. Personnel entering or leaving the area must ensure the entrance or exit point is securely closed.

(3) Visitor Identification and Control. Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's access and need to know. Allow visitors to enter the secure facility for official business only. The SFM approves all visits to their secure facility by non-NARA personnel after confirming their clearance, and access authorization if necessary, with BX (see subpar 3.3b(1)).

(a) Prepare to receive appropriately authorized researchers or other visitors by using NA Form 6052, Checklist for Classified Visits and Meetings, according to par 4.11.

(b) Use a visitor log, showing the visitor's printed name, organization, NARA host name, date of visit, time in, and time out, to record the entry and exit of all visitors. Maintain the logs for two years in accordance with NARA records schedule, item 650-2.

(c) When admitting uncleared visitors to a secure facility, the person admitting the visitors must announce the visitors to other occupants so they may take appropriate actions to secure or cover any exposed classified information. Uncleared visitors must be escorted at all times by appropriately cleared staff to ensure that they do not access classified information.

(d) For visitors with a clearance, the NARA host must validate their clearance, and any controlled access authorization if necessary, with BX, prior to disclosure or discussion of any classified information and consistent with the classification of the material.

(e) An individual with appropriate clearance, and also SCI access (for SCIFs), who is knowledgeable of the security procedures of the secure facility, must continuously escort all non-NARA visitors and NARA personnel who are not similarly cleared or SCI-indoctrinated, while they are in the facility.

(4) Emergency Access. Immediately admit emergency responders and their equipment when they are responding to a medical crisis within the secure facility, without regard to their security clearance status. Escort emergency responders to the degree practical. However, debrief them as soon as possible after the crisis, if appropriate (e.g., in the event of an inadvertent disclosure).

(5) IDS Maintenance Access. Permit IDS maintenance personnel in the facility when repairs or preventive maintenance of the IDS is required. Treat these individuals as visitors (see subpar 4.10c(3)). All maintenance periods must be documented in the IDS.

(6) Entry and Exit Searches. Visually scrutinize visitors to prevent introduction of unauthorized material or equipment into the facility and to prevent the unauthorized removal of material from the facility. Verbally remind visitors to remove and properly secure unauthorized material and equipment before entering the SCIF.

(7) Inspections. Admit authorized inspectors to a secure facility without delay or hindrance when inspection personnel hold the appropriate level of security clearance in accordance with par 3.1 or SCI access for the security level of the facility.

(8) Waste Receptacles. All classified and unclassified papers, consisting of record and non-record, usually operational, material not having permanent retention value must be shredded or placed in red and white-striped classified waste "burn" bags for destruction. Arrange for the destruction of burn bags locally through your ISPM, or at Archives I and II though the Facility and Property Management Division (BF). Mark burn bags as shown in par 7.3. Trash cans may be used only for obvious trash items such as bottles, cans, metal fasteners, tissues, etc.

(9) Closure and Departure. At the close of the business day, or at any time the secure facility will be unoccupied and alternate arrangements have not been made, secure the facility by taking the following action in the order listed to ensure that:

(a) all rooms or spaces in the facility are unoccupied;

(b) all classified information in closed storage areas must be stored inside locked security containers;

(c) all classified information in open storage areas is neatly maintained on desks or shelves within the facility;

(d) all equipment, not authorized for 24/7 operation (servers, etc.) is turned off;

(e) all interior doors in the facility are closed;

(f) an end-of-day check list, SF 701, Activity Security Checklist, or an equivalent form, is completed and initialed when the secure facility is used for operational activities (other than storage only);

(g) the alarm is activated;

(h) the combination lock on the entrance is engaged and checked;

(i) the individual closing the facility completes the SF 702 with his or her initials and the time the facility was closed; and

(j) the monitoring security control station is notified of the closure and confirms that the alarms are active.

NOTE: Maintain the completed SF 701, or an equivalent form, and SF 702 in operational files for at least 3 months following the last entry on the form, in accordance with NARA records schedule, item 259-2.

d. Alarm Response Procedures. If alarm activation occurs, the security control station dispatches an officer to investigate the cause of the alarm. Security uses Part A of the NA 6068 access roster to notify secure facility personnel of the alarm. If the facility appears to be secure and the alarm quickly resets (i.e., nuisance alarm), the notified individual will not be required to respond. However, if the alarm does not reset, the individual must respond when called, during or after work hours, and access the facility to investigate the cause of the alarm. Responding personnel must arrive as soon as possible, but no later than 60 minutes from the time the security control station requested their response. A security officer will remain at the secure facility pending arrival of responding personnel. Upon arrival, the responding individual and security personnel enter and inspect the facility to ensure no unauthorized access has been attempted. If the facility appears to be secure with no attempted access, the responding individual resets the IDS and uses standard closing procedures upon departure. The SFM must notify their ISPM and the ISO of any after hours alarm activations by the next duty day. False alarm rates must not exceed one in a 30-day period per alarm zone.

(1) IDS Testing. After the initial IDS installation and acceptance testing, test the system every six months to ensure the system is functioning properly and maintains an optimum level of performance. Records of the tests must include: testing dates, names of individuals performing the test, specific equipment tested, any malfunctions detected, and corrective actions taken, if applicable. Maintain records of testing and test performance in the facility accreditation folder for two years. Contact BX for assistance in conducting the test.

(2) Response Force Testing. Conduct coordinated response force testing semi-annually, involving only on-site responders. Note the security guard response times and notify BX if not within 15 minutes. Maintain a record of the tests in the facility accreditation folder for two years. False alarm activations may be used in lieu of a response force test provided the required response time is met. BX will conduct response force testing for Archives I and II due to the number of secure facilities in these buildings. IDS equipment testing remains the responsibility of the SFM.

(3) IDS Catastrophic Failure Coverage. If the IDS fails, cleared staff must remain in the secure facility until maintenance personnel can be contacted and respond. Staff may depart when the IDS is repaired and activated.

(a) As an alternative, especially in the case of multiple secure facilities at one location, use a roving guard force performing at least hourly, irregularly spaced, security checks of all secure facility perimeter

doors from the time of system failure until the IDS has been repaired and successfully activated.

(b) Anytime the IDS cannot be immediately repaired, notify your ISPM and the ISO.

(c) ICD 705 also requires that a minimum of 24 hours of emergency backup electrical power be maintained as a first resort for system failures.

(4) Alarm Monitoring and Maintenance Service Contracts. Include in contracts for alarm monitoring and maintenance service, a requirement of minimum response time for repair to the system of two hours during normal business day operations, and four hours outside normal business day operations, including weekends.

e. Emergency Action Plan. SFMs must develop an Emergency Action Plan (EAP) supplementing the overall facility emergency plan for secure areas in which classified information is stored.

(1) The supplemental EAP must provide for the protection or removal of classified information in case of fire, natural disaster, civil disturbance, or terrorist activity, to ensure the information does not fall into the hands of unauthorized persons.

(2) SFMs coordinate the EAP with their building facility managers and incorporate or reference their overall facility emergency plans as much as possible, as they likely already include most requirements. EAPs, including changes, must be submitted to the NARA ISO, through their ISPM, for review and approval before implementation. The EAP may be included in the overall SOP for the secure facility.

(3) Specifically, an EAP for NARA secure facilities, at minimum, includes:

(a) the location of fire extinguishers in or near the secure area;

(b) the location of combinations to any security containers within the secure area;

(c) procedures for admitting uncleared emergency personnel into the area and provisions for safeguarding classified information during such access (see subpar 4.10c(4));

(d) plans for rapid removal of document accounting records to facilitate a possible post-emergency inventory;

(e) emergency evacuation procedures for information, equipment, and personnel;

(f) off-site storage plans and designation of an evacuation site and alternate site;

(g) a requirement to submit a follow-up report to BX as soon as possible anytime EAP procedures are implemented, indicating all actions taken under the plan and the circumstances that caused the plan to be implemented; and

(h) posting emergency signs.

NOTE: According to 29 CFR Part 1910.37(b)(4), if the direction of travel to the exit is not immediately apparent, signs must be posted along the exit route indicating the direction of travel to the nearest exit. Additionally, the line-of-sight to exit signs must be clearly visible at all times.

4.11 Classified Meetings

Additional Procedures for NARA sponsored meetings that involve discussion of classified information, including conferences, seminars, exhibits, symposia, training classes, and other such gatherings:

a. Classified meetings must be held inside a secure facility or other room that has been temporarily accredited or approved for discussion at or above the classification level of the information to be discussed. Coordinate meeting arrangements with the NARA office responsible for the room, or the applicable SFM. Prepare for hosting classified meetings by using NA Form 6052, Checklist for Classified Visits and Meetings.

b. If a secure facility is not available, then:

(1) the meeting locations and security arrangements must be approved in advance by the NARA ISO; and

(2) an individual must be appointed by the NARA meeting sponsor to serve as security manager for the meeting to ensure that cleared NARA government personnel establish and maintain physical security of the meeting site and protect any classified information used or generated during the meeting. Other cleared agency personnel, or contractors with appropriate personnel security clearances, may assist with security requirements for these meetings under the direction of the appointed security manager.

(a) The meeting room must be secured from visual surveillance. Classified information used during the meeting must not be visible to persons outside the room. Cover any windows through which classified information or activities within the meeting room might reasonably be viewed by closing blinds or drapes, or by other means.

(b) The meeting room must be secured from auditory surveillance. If conversations within the meeting room can be heard intelligibly outside the room in uncontrolled areas that are accessible to persons not cleared to at least the classification level of the briefing, the meeting security manager must post cleared individuals outside the room to restrict approaches to the room while the classified meeting is in progress.

c. Keep announcement of the classified meeting unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

d. Segregate classified sessions from unclassified sessions whenever possible.

e. Limit access to the meeting, or at least the classified sessions, to persons who possess the appropriate security clearance and need-to-know. When classified discussions are taking place, the meeting room door must be securely locked and monitored to prevent anyone from entering unexpectedly or without authorization.

f. Visually scrutinize attendees to prevent introduction of unauthorized material or equipment into the meeting room and to prevent the unauthorized removal of material from the room. Follow the guidance on electronic devices in par. 4.13 of this handbook.

g. The meeting sponsor must ensure that classified documents, recordings, audiovisual materials, notes (if not prohibited), and other information created, distributed, or used during the meeting are controlled, safeguarded, and transmitted as required by NARA 202.

h. Meeting participants must dispose of only obvious trash items such as food wrappers, drink containers, metals, napkins, etc., in meeting room trash cans to avoid inadvertent disposal of notes or other papers that may be classified.

i. At the conclusion of the meeting, the appointed meeting security manager must check the room to ensure all materials have been accounted for and nothing has been inadvertently left behind by the meeting sponsor or attendees. File completed NA 6052 checklists under NARA records schedule, item 263-2.

4.12 Individual Precautions

Every NARA employee must take the proper precautions in their daily routines to prevent access to classified information by unauthorized persons by:

a. keeping security containers and other authorized storage facilities locked when not under the direct supervision of an authorized person entrusted with the contents;

b. keeping classified information that has been removed from storage under constant watch and placed face down or covered when not in use;

c. using the appropriate cover sheets for the level of classification applicable to the information in their possession, i.e., SF 703 - Top Secret, SF 704 - Secret, and SF 705 -

Confidential, or the designated cover sheets for controlled access information (available through the ISO);

d. handling classified information stored in or on non-record materials, such as disk media, carbon sheets, plates, typewriter ribbons/cartridges, stencils, stenographic notes, and worksheets by:

(1) destroying them promptly once they have served their purpose (see Chapter 7, Disposal and Destruction); or

(2) marking and protecting them at the same level of classification as the classified information from which they were produced, or derivatively classified, as appropriate;

e. taking precautions to minimize any danger of inadvertently disclosing classified information during conversations, by not discussing classified information in public places, or anywhere outside of areas that have been approved for classified discussions by the proper security authority; and

f.not working with classified information in rooms or offices where uncleared persons are present or where access, visual or auditory, cannot be controlled (see subpar 4.11b(2)(a) and (b)). The use of space dividers is not sufficient to safeguard classified information. While cleared employees are actively working with classified information under their physical control and observation (other than SCI and SAP) it must be, at minimum, in rooms or offices to which access can be controlled or restricted by locked doors and windows. The windows must have blinds, shades, curtains, or similar form of covering, which must be closed while working with classified information to prevent observation of the information from outside. Do not open, read, discuss or work with SCI in any way outside of an accredited SCIF. SAP information must only be handled within facilities approved by the SAP owner's PSO, or a SCIF that is dual-accredited for both SCI and SAP under a signed agreement between the cognizant security authority for the SCIF and the PSO.

4.13 Portable Electronic Devices

The following policy on the use of Portable Electronic Devices (PEDs) is applicable to all personnel working in or visiting any NARA secure facility. The technological capabilities and portability of PEDs raise security concerns that are particularly relevant to secure facilities. Consequently, all PEDs used within or introduced to NARA secure facilities must meet the minimum security requirements outlined below. Do not presume that new developments in technology or capabilities that are not specifically addressed in this handbook constitute approval for their use. Instead, seek further guidance from the NARA ISO before introducing the device into a secure facility. Access to a secure facility may be denied and PEDs may be seized or held for inspection by the SFM or BX for failure to comply with these prohibitions, and violators could be subject to the sanctions cited in section 5.5 of E.O. 13526.

a. The following PEDs are NOT permitted in NARA secure facilities:

(1) Unofficial PEDs (except those listed in subpar 4.13c);

(2) Two-way transmitting devices such as cellular telephones, smartphones, Bluetooth devices, and two-way pagers;

(3) Recording devices (such as MP3 players, still and video cameras) that have any photographic, audio, video, or optical recording capability, including all associated media;

(4) Data storage devices such as Universal Serial Bus (USB), FireWire, and PCMCIA devices, to include thumb drives, data wrist watches and all other plug-and-play devices capable of storing data;

(5) PEDs that have infrared (IR), radio frequency (RF) or other wireless capability. Communications attachments (e.g., local area network (LAN) cards and modem cards) must also be removed from PEDs before entering the secure facility; and

(6) Smartphones, tablet computers, e-Readers, phablets, Personal Digital Assistants (PDAs), and other digital devices, such as an iPhone, iPad, iPod, Kindle, Galaxy Note, Palm Pilot, Pocket PC or Compaq iPAQ may not be used or approved for processing or storage of classified information or for connection to classified IT systems.

b. The following items are permitted on a limited basis (by time or scope) only if issued by NARA and required to perform official duties:

(1) Certain types of two-way transmitting equipment, such as two-way radios (walkie-talkies);

(2) Recording equipment (audio, video, optical). Any associated media must be appropriately controlled by the SFM;

(3) Universal Serial Bus (USB), FireWire, and PCMCIA data storage devices to include thumb drives, MP3 players, cameras, and other plug-and-play devices capable of storing data when specifically approved in advance by the ISO and prohibited features have been mitigated. If explicit permission is obtained for entry and exit of data storage devices to and from NARA secure facilities, handle those devices as specified upon approval, or as removable media, according to par. 4.14, when crossing secure boundaries; and

(4) Government-owned unclassified laptops configured to meet minimum technical security requirements to disable digital, audio and image recording and infrared (IR) capabilities, and with explicit written permission from the ISO.

c. The following PEDs may be introduced into the secure facility:

(1) Personally owned medical devices;

(2) Electronic calculators, electronic spell checkers, wrist watches and data diaries without USB or other data interfaces;

(3) Receive-only pages and beepers, audio and video equipment with only a playback feature (no recording capability) or with the record feature disabled/removed;

(4) PEDs that have only IR wireless capability or IR ports, and the IR feature is disabled; and

(5) Government-owned classified laptops configured according to subpar 4.13b(4), or ICD 503 when used in SCIFs.

d. Admit TEMPEST and Technical Surveillance Countermeasures (TSCM) equipment into secure facilities as long as the personnel operating the equipment are certified to do so and have the appropriate security clearance and access indoctrination.

4.14 Protection of Media

a. Classified media must be identified, labeled and safeguarded in a secure environment (i.e., security container or an approved secure facility), as appropriate to the amount of material and the level of its original classification. See par. 2.6g regarding labeling requirements. Once either classified or unclassified media has been introduced into a secure environment, it must remain there until an appropriate declassification or content review has been conducted or the media is destroyed.

b. Media that remains classified may be transmitted between secure environments in accordance with the procedures in Chapter 5 of this handbook.

c. Media that is unclassified, declassified, or downgraded (in classification level) and has been stored within a secure environment, or output extracted from any classification of media that is stored in a secure environment, must be reviewed for content before it may be removed from that environment.

(1) Human-Readable Output Review. Electronic output from classified media or unclassified media stored within a secure environment that is to be taken outside the security boundary where the media is stored, must be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footers) before being removed.

(2) Media Review. Information on media that cannot be reviewed in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. Random or representative sampling techniques approved by the appropriate cognizant security authority for the type of classified media involved may be used to verify the proper marking of large volumes of output.

(3) Identification. The reviewer must ensure all media output that has been examined and approved for removal outside the secure environment of its source is clearly and accurately marked as unclassified, or with the appropriate classification or declassification markings, as appropriate, in accordance with par. 2.6 of this handbook.

d. Media that has been approved strictly for extracting information from environmental systems, such as a data logger, cannot be left in the secure environment and can only be brought into the secure environment strictly for downloading environmental data and immediately taken back out of the secure environment. This media must not be used with any other piece of equipment or information technology system, prior to, during, or after being used with the data logger.

[Return to TOC]

Chapter 5

TRANSMISSION

5.1 General

Classified information must be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be prevented, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with 32 CFR Part 2001.

5.2 Transmission Within NARA Facilities

a. Classified information transmitted from one storage area to another, between offices, or to other personnel situated within the same NARA facility must be hand carried in closed containers only by properly cleared individuals. Place the appropriate cover sheet on top of the classified document and insert it into an opaque envelope or other appropriately sized container. Remove the envelope or container once the document has been moved. Leave the cover sheet attached to the document until action is taken on the document or it is filed in a security container. Receipts are not required for non-accountable classified information transmitted within the same facility.

b. Individuals transmitting classified information within a NARA facility must not carry classified documents into public areas such as cafeterias, shops, auditoriums, exhibit areas, gymnasium, while en route to their destination.

c. Uncleared personnel may move closed containers containing classified information provided they are continuously supervised by a properly cleared NARA employee.

d. In the event of a drill or actual emergency, NARA employees and contractors are still obligated to make every effort, without endangering human life or safety, to properly secure classified information they are in the process of transmitting before exiting the building. If it cannot be returned to its normal location, the transmitting individual should store it in the nearest available secure facility, classified stack, or safe. If that's not possible due to life/safety concerns, and the information is small enough to hand carry, the individual should exit the building and keep the information on them at all times and remain in the immediate area until allowed back in the building. If proper storage is not possible due to life/safety concerns, and the information is bulky, the individual should store it in the nearest lockable stack, vault, safe, cabinet, or office and exit the building as quickly as possible. Once the emergency condition is over, the individual must immediately return to the location where the information was temporarily stored, notify your ISPM, the ISO and the NARA staff responsible for the area, and thoroughly check the information to verify no tampering or loss has occurred.

5.3 Transmission Between NARA Facilities

a. Classified information transmitted between separate NARA facilities must be either hand carried by an authorized courier in accordance with par. 5.9, or dispatched as you would to addressees outside NARA (par. 5.4) via any of the approved transmission methods outlined in this chapter, as appropriate for the classification and category of the information being sent.

b. Receipts are not required for non-accountable classified information that is hand-delivered directly to an authorized recipient in another facility under NARA's control. When using any other method of transmission, use a document receipt (par. 5.5) to ensure control of the information is maintained during transit between facilities.

5.4 Transmission Outside NARA Facilities

Classified information transmitted outside NARA facilities may be dispatched via any approved method outlined in this chapter, as appropriate for the classification and category of the information being sent. Receipts are always required, except as specified in par 5.5c.

a. Envelopes or Containers. All the seams of an envelope or wrapper must be sealed with tamper-resistant tape, such as fiber-reinforced brown paper tape, plain brown postal tape, or otherwise packaged in a manner designed to provide tamper indication (e.g., by using lockable briefcases or security courier pouches) to prevent undetected access to the contents while in transit.

(1) When classified information is transmitted outside NARA facilities, it must be enclosed in two opaque envelopes, if size permits, or similar wrappings or containers that conceal the contents and provide reasonable evidence of tampering.

(2) The classified information must be protected from direct contact with the inner container to avoid classified print rubbing off onto the inside of the container. One way to do this is by placing a cover sheet on the front of the document and a sheet of paper or cover sheet to protect the back of the document if the document has information on the back page.

(3) Classified material of a size not suitable for packaging in accordance with subpar 5.4a(1) above must be enclosed in two sealed opaque containers, such as boxes or heavy wrapping. Special shipping containers including closed cargo transporters may be used instead of the above packaging as one of the two containers. In such cases, the shipping or cargo container may be considered the outer wrapping or cover. This container must be of sufficient construction to provide evidence of forced entry, secured with an HPT approved key or combination padlock, and equipped with a numeric security seal that would provide evidence of entry. See par. 5.9d(5) for hand carrying large items or quantities locally.

(4) Material used for packaging must be strong and durable enough to provide security protection while in transit, to prevent items from breaking out of the envelopes or containers. Materials should facilitate the detection of any

tampering of the contents. Seal bulky packages or large containers with brown fiber-reinforced paper tape or tamper-evident security tape.

b. Addressing. Address envelopes or packages containing classified information only to official Government offices or U.S. contractors with a facility clearance. The addressee must have appropriate storage capability and the container must show the complete return address of the sender. The term "container" as used in the following paragraphs refers to any form of packaging for classified information.

(1) Inner Containers:

(a) The inner container must show the address of the sending and receiving offices, the highest classification of the contents (front and back – top and bottom), including any controlled access markings or caveats, and any special instructions. It must be carefully sealed with tamper-resistant brown paper tape.

(b) The name of a person may be used in the address on the inner container; however, position titles or office codes or phrases such as "Attention: Security Officer" are recommended. When addressed to a specific individual, the sender should ensure that the person is still at the address and verify through the NARA Personnel Security Officer that he or she holds the necessary clearance.

(c) Package the material so that classified text is not in direct contact with the inner envelope or container. NA Form 2011, Classified Document Control Record, or other NARA-produced receipt for the material, must be enclosed in the inner container or otherwise accompany the material as required in par. 5.5.

(2) Outer Containers:

(a) The outer container must not bear any classification markings, list of contents, or any other information or marks that might indicate that the contents are classified.

(b) The outer container must show the complete, correct address of the recipient and the return address of the sender. Containers to be delivered by messenger or courier must show complete street address and room number. The outer container may also be addressed to an individual; however, the concerns described in subpar 5.4b(3) should be taken into consideration before doing so. Again, office codes or phrases such as "Attention: Operations Division" should be used.

(c) Classified information intended only for the U.S. elements of international staffs or other international organizations must be addressed specifically to those units.

(3) When classified material is received in the mail, it must be quickly processed and given the appropriate protections. In many cases, if packages are received with a name on the envelope, it might be placed in that individual's distribution bin or left on their desk, in unsecure areas, even if that person is on vacation. This could lead to classified information sitting for long periods unsecured. Additionally, when an envelope is addressed to an individual, others may tend to shy away from opening the envelope because of "privacy" concerns. There are some cases when names might be necessary, but the sender should be judicious when using them. It should be the exception, rather than the rule. The sender should ensure that, when addressing a classified package to an individual, the person is still assigned to the organization and will be there to receive the mail, or whenever it is requested by the receiving organization. (Some organizations have their classified mail sent to a post office box, addressed under an individual's name, in order to mask sensitive associations and restrict distribution.)

5.5 Receipt Systems

a. Receipts must be provided by the sender of the material and enclosed in the inner container. If not practical, the receipt may be sent to the recipient with an advance notification of shipment, or may be hand-carried when delivered by courier as outlined in par 5.9.

(1) Receipt forms must be prepared in triplicate and remain unclassified when completed. Two copies of the receipt must be placed in the inner container with the material (except as noted above) when sent to the intended recipient. The third copy must be maintained by the sender until the original is signed and returned.

(2) The sender must make sure that the receipt is returned by the addressee within a reasonable time, but no later than 30 days after dispatch. If not received within the prescribed time period, a tracer (consisting of a copy of the receipt, stamped or marked “TRACER – SIGN AND RETURN IMMEDIATELY”) must be sent to the addressee. Make telephone contact to verify delivery of both the original material and the receipt(s). If a signed receipt is not provided within a maximum of 60 days from dispatch, report the situation to the ISO as a security incident for further investigation.

b. Top Secret and Secret information must be controlled under a continuous chain of receipts when transmitted outside of NARA facilities, to provide sufficient documentation to investigate any loss or compromise.

c. Receipts for Confidential information are not required except when the information is transmitted to a foreign government (including foreign government embassies and consulates located in the United States) or upon request. However, if a receipt is enclosed it must be signed and returned to the sender.

d. Use NA Form 2011, or other NARA-produced document receipt, for classified information dispatched from NARA facilities.

e. NA Form 14044, Change of Status Record – Record Group Level, or SF 135, may be sent with classified information being transmitted to another NARA depository in place of NA Form 2011 if the information supplied on these forms provides the same level of documentation as the NA 2011.

f.NA Form 14014, Loan Receipt for the National Archives, may be used as a courier or container receipt for packages that contain classified information, but only in addition to the NA Form 2011 receipt for the classified information itself. A person authorized to accept delivery for the addressee signs the NA 14014 and makes internal distribution to the intended recipient, who, after opening the package and verifying the contents, signs the NA Form 2011 and mails it back to the sender.

g. Facsimile Transmission. Individuals transmitting classified information through secure facsimile systems must confirm receipt (verbally or in writing) with the intended recipient.

(1) Fill out and transmit an NA Form 2011 with the classified information, or use the fax cover page instead of the NA Form 2011, if it sufficiently identifies the information being transmitted. Upon receiving the fax, the recipient completes the receipt or signs the cover page and immediately returns it by fax.

(2) Alternatively, you may contact the intended recipient and notify him or her that classified information is being transmitted by fax. Upon receipt, the recipient must telephone the sender to verify the complete transmission was received. Document this verbal communication and retain as a receipt.

h. Maintain receipts for 2 years in accordance with NARA records schedule, item 253.

5.6 Methods of Delivery by Classification or Category

a. Top Secret information must be transmitted by one of the following means:

(1) Direct delivery to authorized persons within a NARA facility. An NA Form 2011 receipt is not required.

(2) NSA, State Department, CIA, or DOE courier systems.

(3) Defense Courier Service (DCS).

(4) One or two, as appropriate, cleared and appointed NARA employees possessing an NA Form 6028, Courier Authorization, when transporting the information between or outside of NARA facilities in the same local area by any mode of transportation, or two cleared couriers when transporting elsewhere within the United States in a land-based vehicle owned, controlled, or chartered by the Federal Government.

(5) One or two, as appropriate, cleared and appointed NARA employees possessing a courier authorization badge (NA Form 6028) and an official courier authorization letter, signed by the cognizant ISPM or the NARA ISO, when transporting the information within the United States by commercial aircraft or other modes of transportation that require the courier to pass through inspection checkpoints. One person may serve as a courier; however, the authorizing official must assess circumstances such as volume of material, mode and length of travel, high crime area, sensitivity, etc., which would indicate that more than one person would be prudent to ensure continuous custody and protection of the material.

(6) A cryptographic system authorized by the Director, National Security Agency, to process Top Secret information, or a protected distribution system designed and installed to meet standards included in the National Communication Security (COMSEC) and Emanations Security (EMSEC) issuance system. Secure fax machines located within NARA secure facilities meet the definition of such a system.

NOTE: Top Secret information may not be transmitted under any circumstances via the U.S. Postal Service (USPS) or other private carriers (e.g., United Parcel Service (UPS), Federal Express (FedEx), Panther, Landstar, or Boyle Transportation, etc.). No classified information of any sort may be transmitted over unsecured telephone, fax or electronic mail systems.

b. Secret information must be transmitted by one of the following means:

(1) Any of the approved means for the transmission of Top Secret information can be used to transmit Secret information; however, Secret information may only be introduced into the DCS when the information cannot otherwise remain under U.S. control.

(2) USPS registered mail (or USPS Priority Mail Express Next Day Delivery when approved by the cognizant ISPM) for transmission of Secret and Confidential information within the continental United States. Material must be introduced into the postal system "across-the-counter" at a USPS facility; use of postal drop boxes is prohibited. The ISPM must not approve dispatch of USPS express mail overnight shipments on Fridays, or when the next day is a holiday, to avoid packages remaining overnight or over the weekend in USPS facilities. When filling out the express mail (USPS Label 11-B or 11-F), be sure to select the option that requires the US postal carrier to obtain a signature from the recipient. Pay attention to which edition of the 11-B or 11-F label you are filling out. Editions older than January 2012 require postal carriers to obtain a signature by default (so do <u>not</u> check the waiver box). However, you must be certain to check the "signature required" box on newer labels.

(3) USPS registered mail through Army, Navy, or Air Force postal service facilities outside the United States provided the information does not at any

time pass out of U.S. citizen control and does not pass through any foreign inspection or postal system.

(4) Commercial express carrier in accordance with par. 5.7 of this handbook.

(5) Common or Contract Carrier in accordance with par. 5.8 of this handbook.

c. Confidential information must be transmitted by one of the following means:

(1) Any of the approved means for the transmission of Secret information can be used to transmit Confidential information.

(2) USPS certified mail within the continental United States.

(3) USPS first class mail within the continental United States, when the destination is a U.S. Government facility and the outer container is stamped **FIRST CLASS** and **POSTMASTER: DO NOT FORWARD - RETURN TO SENDER**. Postal inspection is avoided if the outer wrapping is marked **FIRST CLASS**. If a piece of first class mail weighs over 12 ounces, it must also be marked **PRIORITY MAIL**. These markings are necessary because outsized mail, unless readily identifiable as first class mail (which is closed to postal inspection), can be mistaken for a lower class of mail and may be subject to postal inspection. The use of street side mail collection boxes is prohibited.

(4) Use USPS registered mail for Confidential information transmitted to U.S. Government facilities located outside the United States.

d. Restricted Data/Formerly Restricted Data (RD/FRD) information must be transmitted in accordance with DOE Order 471.6, Information Security. RD/FRD documents may be prepared and transmitted by the same means as other classified information at the same security classification level, including overnight shipments by USPS and commercial express carriers. Make sure the inner container bears the restrictive "Contains RD/FRD Material" markings.

e. Sensitive Compartmented Information (SCI) may be transmitted only by certified NARA or other agency couriers who are designated and authorized to hand carry SCI, the DCS, or by secure fax approved for that purpose. SCI must be transmitted from one SCIF to another in accordance with ICD 703 to ensure it is properly protected. SCI must be prepared by SCI indoctrinated personnel in the same manner of packaging as other classified information at the same security classification level. In addition to the requirements of pars 5.4 and 5.5, the inner container will be stamped or annotated with the notations "**TO BE OPENED BY THE SPECIAL SECURITY OFFICER**" immediately above the destination address and "**CONTAINS SENSITIVE COMPARTMENTED INFORMATION**" placed below and to the left of the destination address and on the reverse. Material hand carried by a courier must be marked, on the outer container only, with a notation similar to the following example; below and to the left of the destination

address (must reflect the dispatching NARA facility's address and a telephone number that is staffed at all times):

PROPERTY OF THE US GOVERNMENT
TO BE RETURNED UNOPENED TO:
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
SECURITY CONTROL CENTER
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740
(301) 837-2900

f.SAP information must be transmitted by the same means approved for the transmission of SCI. It must be prepared, reproduced and packaged by SAP indoctrinated personnel in SAP accredited facilities. In addition to the requirements of pars 5.4 and 5.5, the inner container will be stamped or annotated with the notations "HANDLE VIA SPECIAL ACCESS CHANNELS ONLY" immediately above the destination address and "SPECIAL ACCESS REQUIRED" placed below and to the left of the destination address and on the reverse. SAP transmissions must strictly follow the addressing protocols established by the PSO for both the outer and inner containers to ensure the information is received only by appropriately cleared and indoctrinated personnel. Contact the responsible PSO for the appropriate address to use when transmitting SAP information.

g. North Atlantic Treaty Organization (NATO) classified information must be transmitted under the guidelines contained in USSAN Instruction 1-07. NATO has established a central distribution point for the receipt and distribution of NATO documents within each NATO member nation. The central distribution point for the United States is the Central U.S. Registry (CUSR) located at the Pentagon. NARA sub-registries and control points (currently National Declassification Center [ANDC], George Bush Library [LP-GB], Ronald Reagan Library [LP-RR], William J. Clinton Library [LP-WJC], George W. Bush Library [LP-GWB], and Dwight D. Eisenhower Library [LP-DDE]) receipt, control and distribute all NATO classified information at NARA. **COSMIC Top Secret, NATO Secret, NATO Confidential** and all **ATOMAL** documents must be transferred through the registry system and be double-wrapped in the same manner as equivalent U.S. classified documents, except that the inner container must be marked with the appropriate NATO markings. Documents marked **NATO Restricted** must be packaged in the same manner as **NATO Confidential** and above. The outer container must be marked **POSTMASTER: DO NOT FORWARD - RETURN TO SENDER** and may be transmitted via first class mail. NATO classified information may not be transmitted via commercial express carrier.

h. Communications Security (COMSEC) material must be transmitted and transported in accordance with NSA/CSS Policy Manual 3-16 or CNSSI-4005. Controlled COMSEC may not be transmitted via commercial express carrier.

i.Foreign Government Information (FGI). Transmittal of FGI, including preparation, classification markings and methods of transmission is the same as prescribed in this chapter for all other classified information of the same classification level (also see subpar 4.4f), with the following exceptions:

(1) The release or disclosure of foreign government information to nationals or any entity of a third-country must have the prior written consent of the originating government.

(2) FGI may not be transmitted via commercial express carrier.

5.7 Transmission by Commercial Express Carrier

The use of commercial express carriers for overnight shipments of classified matter is restricted to Secret and Confidential information in emergency situations when the information positively has to be at the receiving facilities on the next working day. Use of USPS registered and first class mail is the standard method of delivery for Secret and Confidential information, respectively, between NARA components. Commercial express service must not be used as a matter of routine or convenience for transmitting classified matter. Controlled Communications Security (COMSEC) information, NATO, and FGI may not be transmitted via commercial express carrier.

a. United Parcel Service (UPS) is currently approved to provide overnight carrier service for Government classified shipments under contract with GSA. UPS Express "Next Day Air Early AM", "Next Day Air", and "Next Day Air Saver" services are the only authorized delivery options for classified material; however, the "Saver" option may only be used if you have confirmed that the intended recipient will be available as late as 5:00PM at the destination site, since the guaranteed delivery times are as late as 3:00 to 4:30PM. Use of UPS Ground for shipment of classified information is prohibited. Other commercial carriers (e.g., FedEx Express (not FedEx Ground), DHL, Airborne Express, etc.) may be used for shipment of classified information when:

(1) requested and paid for by the addressee; and

(2) use of the alternate carrier meets or exceeds delivery times and the sender complies with all other shipping requirements in this par (5.7a through f).

b. The sender must verify the mailing address and make sure, before dispatching, that an authorized person will be available to receive and secure the material at the delivery destination. Do not use overnight service on Fridays or on the day preceding a holiday, unless previous written assurance has been received from the intended recipient that someone will be available to receive the shipment upon arrival at their location. This is to avoid packages remaining overnight or over the weekend in carrier facilities.

c. The commercial express carrier envelope is not considered the outer (second) container for double-wrapping requirements; therefore, the package must be double-wrapped with all seams sealed using brown paper fiber-reinforced or postal tape, then placed into the carrier envelope, which becomes a third container. The document(s) and the inner (first) container should be stamped top & bottom, front & back, with the classification. You also need to fill out a receipt (NA Form 2011) or other NARA-produced document receipt and place it inside the inner container for the recipient to sign and return to you. Both the inner (first) and outer (second) containers should also have the return and destination addresses, but the outer (second) container must not be stamped with any classification markings. The double-wrapped package then is placed inside the express mailer (third container) for

dispatch. It is not necessary to use extra tape on the express carrier envelope. The carrier's packaging is not required to be sealed with tape like that required for the enclosed envelopes containing the classified information. The carrier packaging, without extra tape, assures that classified information is not outwardly identifiable as such during shipment.

d. The express carrier envelope may be addressed to the recipient by name; however, the signature release block on the receipt label (authorizing delivery without it being signed for) must not be executed under any circumstances. Material must be delivered "across-the-counter" at a carrier facility or hand delivered to a carrier representative in sufficient time to allow for dispatch on the same day; use of drop boxes is prohibited. All classified information dispatched via commercial express carrier must meet the carrier's standard size and weight limitations. Do not identify the shipments as containing classified information, neither by telling carrier employees nor by marking the express carrier envelope.

e. The sender must track each package via the internet-based tracking service. However, tracking is not a substitute for a document receipt. Upon delivery, the package may be signed for by mailroom personnel for internal distribution to the authorized recipient. Since tracking may only show delivery to the mailroom, it doesn't give you the verification you need that the classified contents were actually received by the intended addressee and properly secured. The NA Form 2011 or equivalent, once signed and returned to you by the addressee, will serve this purpose.

f.Report any problems with commercial express carrier delivery of classified matter, including shipments not delivered in the specified timeframe, in accordance with the procedures in Chapter 9 of this handbook for reporting security incidents.

5.8 Transmission by Common or Contract Carrier

The use of common commercial carrier services for transporting classified matter is restricted to Secret and Confidential information. Common carrier services include all modes and means of transport (e.g., air, rail, vehicular), excluding commercial express carriers discussed in par. 5.7. The following requirements apply to the use of such commercial services, as well as bulk shipments of classified matter.

a. Preparation and Notifications:

(1) Contract carriers (for example, trucking companies such as Panther, Landstar, or Boyle Transportation, etc.) holding industrial facility and personnel security clearances through the Defense Industrial Security Clearance Office (DISCO) must provide, through their Facility Security Officer (FSO), copies of the clearance approval forms to the Security Management Division (BX) for their facility and each of the contract personnel who may be handling the material, before accepting a classified shipment.

(2) BX verifies the clearance information and provides results to the releasing office before shipment. Clearances must be equal to or higher than the

material to be shipped by this method, which is limited to Secret and Confidential information.

(3) When the contract carrier does not have the appropriate clearances through DISCO, or records of a higher classification than Secret need to be transported, cleared NARA employees accompany the shipment in accordance with par. 5.9. In either case, carriers may not stop overnight during the transport of the material.

(4) The receiving location must be notified of the shipment before its departure, with sufficient time to enable proper handling at the destination. At a minimum, the notification must include the nature of the shipment, means of shipment, lock combinations and security seal numbers, anticipated time and date of arrival, an NA 2011 or equivalent receipt for the recipient to sign upon arrival of the shipment, and a request for immediate return notification if the shipment is not received by the estimated time of arrival furnished by the originating NARA office. Upon receipt of such notice, the originating NARA office must immediately notify the NARA ISO and begin tracing the shipment.

(5) Contents must be securely packaged in compliance with this handbook and Interim Guidance 1702-1, Freight Transport of Records and Holdings in NARA's Legal and/or Physical Custody. Bulk palletized shipments must be shrink-wrapped on the top and all four sides. Tamper evident security tape must be applied on top of the shrink-wrapping, over the top center and down each side of the pallet.

(6) Cargo containers or the closed cargo areas of vehicles, vans, trucks and railroad cars used for transporting classified information must be secured with security seals in a manner to show evidence of tampering. Seals must have serial numbers, which must be entered on bills of lading or other shipping papers and emailed to the receiving location. Seal numbers must be verified by the consignee upon arrival of a shipment. The container or cargo area must also be secured with an HPT approved key or combination padlock. The padlock key or combination is known to, and provided from the releasing office to the receiving office location only.

(7) While enroute or at the destination, if the shipment shows any signs of tampering, if a seal is broken, seal numbers do not match, or a lock missing or damaged, the discovering individual must immediately notify the originating NARA office or responsible ISPM. Upon receipt of such notice, the originating NARA office or ISPM must immediately notify the NARA ISO following the security incident reporting procedures in Chapter 9 of this handbook.

b. Protective Measures:

(1) Sufficient personnel with appropriate clearance, and access authorization if applicable, must be tasked for each movement to ensure continuous protection of the matter being transported. Contract carriers or the responsible NARA originating office must provide no less than two cleared personnel to handle each shipment.

(2) While in transit, the common carrier service must provide:

(a) dual driver protective service by carrier employees with appropriate clearance equal to or higher than the material to be shipped by this method, which is limited to Secret and Confidential information;

(b) a Global Positioning System (GPS) or other system that ensures prompt tracking of the shipment while en route; and

(c) arrangements with a cleared U.S. Government or contractor facility that has the requisite storage capability, when emergency storage is required.

(3) When shipments are transported by rail, cleared NARA or contract personnel escorting the shipments must travel in an escort rail car accompanying the shipments, keeping the shipment cars under observation. When practical, as time permits, personnel escorting shipments must check the cars, container locks, and tamper-indicating devices. Escort personnel act as liaisons with train crews, other railroad personnel, special police, and law enforcement agencies, as appropriate.

(4) When shipments are transported by motor vehicles, personnel escorting the shipments must maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the cargo and take appropriate action, as circumstances require, avoiding situations that may interfere with the continuous safe passage of the vehicles. During short stops or breaks, personnel escorting shipments must check the tamper-indicating devices and locks.

(5) The identity and clearance authorization of persons who receive and sign for classified matter must be verified.

5.9 Transmission by NARA-Appointed Couriers

The NARA ISO may authorize NARA employees to hand carry classified information between or outside of NARA facilities, anywhere within the United States and its territories, by issuance of an NA Form 6028, Courier Authorization. Employees must hold a security clearance equal to or exceeding the classification level of the information to be hand carried.

a. Request for Appointment. ISPMs may request that appropriately cleared NARA employees with a valid need to perform courier duties be authorized to escort or hand carry classified information. In accordance with subpar 5.9b, BX issues an NA Form 6028 to

these individuals, who must comply with all provisions of this chapter, as applicable, when transporting classified information.

b. Courier Authorization Badge:

(1) The NARA courier authorization badge (NA Form 6028), authorizes the bearer to transport or hand carry classified information on a recurring basis. The badge identifies the holder by name, card number and includes a current photograph. The badge provides notice that the courier is authorized to carry classified information up to a specific level, specifies an expiration date, and carries the signature of the issuing BX security official. The courier must sign a statement on the reverse side of the badge acknowledging that they have been briefed on their responsibilities as a courier of classified information by their cognizant ISPM or the NARA ISO. The courier badge also lists a 24-hour telephone contact number in the event of an emergency.

(2) BX maintains accountability of all courier authorization badges. Only the ISPM may request the issuance of a courier authorization badge for personnel under their cognizance, after briefing the intended bearer on NARA courier policy and responsibilities using NA Form 6049, U.S. Government Courier Instructions and Briefing Acknowledgement. Send signed forms to the ISO. The ISO may authorize issuance of a courier badge for individuals who do not have a designated ISPM. Other data may also be required to issue the badge, such as a digitized photo and/or signature of the employee. Upon verification of the employee's security clearance and a valid courier requirement, BX issues the badge to the employee. The NA 6049 will be maintained under item 262 of the NARA Records Schedule.

(3) The level of classified information an employee is authorized to carry cannot exceed their own personnel security clearance level (individual security clearance), but it may be lower, depending on the needs of the requesting NARA office.

(4) The bearer of the courier authorization badge must immediately report the loss or damage of the badge in writing to their ISPM or the NARA ISO. The bearer may request a replacement card. The loss of a courier authorization badge may result in forfeiture of courier privileges for an unspecified period of time, or other disciplinary action, as determined by the individual's supervisor, ISPM and/or the ISO.

(5) The bearer must return the courier authorization badge to their supervisor or ISPM upon termination employment with NARA, termination or suspension of his or her security clearance, when authorization is no longer needed, or when any other occurrence dictates the need to withdraw the courier authorization, as determined by the individual's supervisor or BX.

(6) The courier must not use the courier authorization badge for purposes other than its intended use. Abusing or exceeding the authority of the card may result in disciplinary action.

c. Courier Authorization Letter:

(1) Anytime a bearer of a valid courier authorization badge must transport classified information via commercial aircraft, or other modes of transportation that require the courier to pass through inspection checkpoints, they must obtain an official courier authorization letter, signed by the cognizant ISPM or the NARA ISO, before traveling. See the NARA ISO or the Safety, Security & Emergency page of the NARA@work web site for an example.

(2) Before departure, a copy of the courier authorization letter must be left with NARA Security Control, or other 24-hour NARA point of contact identified in the letter, so they may provide verification when necessary. The authorization letter must be delivered in person, or sent via fax or e-mail and followed by a phone call to ensure that it has been received.

(3) The courier presents the original copy of the courier authorization letter, as necessary, to transportation carrier officials to allow uninhibited passage through passenger checkpoints. A reproduced copy is not acceptable; however, the traveler must carry sufficient legible copies to provide to each carrier involved, if requested. The letter is prepared on NARA letterhead stationery and:

(a) provides the full name of the individual and employing agency (i.e., NARA);

(b) describes the type of identification the individual present (for example, NARA courier badge and state driver's license) and ID number;

(c) describes the material being carried (for example, one locked briefcase with three 9x12" sealed packages containing paper documents, and one sealed 6x9" package containing a computer hard drive);

(d) identifies the point of departure, destination, and any known transfer points;

(e) shows the date of issue and includes an expiration date;

(f) carries the name, title, and signature of the cognizant ISPM or ISO issuing the letter; and

(g) indicates the name and official telephone number for NARA Security Control, or another NARA 24-hour point of contact that can verify the validity of the letter.

d. General Escort or Hand Carrying of Classified Information. Individuals authorized to hand carry classified information must:

(1) hold a personnel security clearance equal to, or higher, than the information they are required to transport;

(2) read and sign NA Form 6049 upon issuance of their courier badge, and each time classified information is transported by commercial aircraft or other modes of transportation that require the courier to pass through inspection checkpoints;

(3) possess a valid courier authorization badge and carry it on their person at all times while transporting classified information;

(4) obtain an official courier authorization letter when transporting the information via commercial aircraft or other modes of transportation that require the courier to pass through inspection checkpoints;

(5) prepare the classified information in accordance with pars. 5.4 and 5.5;

(6) in lieu of or in addition to the outer container, use a locked courier pouch, locked briefcase, or the:

(a) passenger or open cargo areas of a locked government vehicle that are continuously viewable and accessible to the courier; or

(b) closed cargo area of a government vehicle, which if *not* continuously viewable and accessible to the courier, are secured with numeric seals and an HPT approved padlock;

(7) not read, study, display or use classified information in any manner when traveling in public conveyances or places, nor leave the information unattended;

(8) not store classified information in a detachable storage compartment such as an automobile trailer, luggage rack, aircraft travel pod, or drop tank, when carried in a private, public, or government conveyance;

(9) comply with the storage provisions of Chapter 4 and this section for all stops en-route to the destination; otherwise, the information must be retained in the physical possession and constant surveillance of the individual at all times (see NOTE below); and

(10) obtain a signed receipt for the information, when required, from an authorized recipient who holds sufficient clearance to accept it. Use NA

Form 2011, Classified Document Control Record, or other NARA-produced receipt, in accordance with pars 5.3 through 5.5 of this handbook.

NOTE: Hand carrying classified information on trips that involve an overnight stop is prohibited without advance arrangements for proper overnight storage in a U.S. Government facility or a cleared contractor's facility that has the requisite storage capability.

e. Hand Carrying Classified Information Aboard Commercial Transportation:

(1) Classified information may be hand carried aboard commercial passenger aircraft or other modes of transportation that require the courier to pass through inspection checkpoints when:

(a) it is the only means available to move the information in the time required to accomplish operational objectives or contract requirements;

(b) specifically authorized in writing, in the form of an official courier authorization letter, signed by the cognizant ISPM or the NARA ISO; and

(c) aboard a U.S. carrier. Use of foreign carriers may be used only when no U.S. carrier is available and authorized in writing by the NARA ISO. The approving official (ISPM or ISO) and the courier must ensure that the information remains in the custody and physical control of the courier at all times.

(2) The ISPM or ISO signing the courier authorization letter signs each outer container on its face to verify proper packaging and signify to transportation officials that the material is to be exempt from inspection.

(3) The packaging for classified information must not contain metal bindings and must be prepared in accordance with par. 5.4; however, the double-wrapped material must be further placed inside a locked briefcase or similarly strong, locked carry-on bag. The briefcase or bag must not be outwardly identifiable to other passengers as containing classified information. The briefcase or luggage holding the packaged information may be opened for routine inspection for weapons. The screening officials may check the packaged material by X-ray machine, flexing, feel, and weight, but must not open the packages themselves.

(4) Persons carrying classified information should process through ticketing and boarding procedures the same as all other passengers, following the courier instructions contained in NA Form 6049.

(5) Classified information in sealed or packaged containers too large to hand carry must be processed as follows:

(a) The NARA official who authorized the transport of the classified information must notify the appropriate transportation carrier in advance.

(b) The courier escorting the information reports to the ticket counter before boarding, present documentation and the classified container(s). A transportation representative reviews the documentation and description of the container(s).

(c) If transportation officials are not satisfied with the identification of the courier or the documentation, the courier should not board, immediately contact their ISPM or the NARA ISO, and not subject the container(s) to further examination.

(d) If satisfied with the identification and documentation of the courier, a transportation official escorts the courier to the screening station where the container(s) are screened.

(e) A transportation carrier representative supervises the actual loading and unloading of the material; however, appropriately cleared NARA personnel must accompany the material and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared NARA personnel must be available to conduct surveillance at any intermediate stops where the cargo compartment is to be opened. Information on any such stops must be obtained from the transportation carrier when notifying them of the courier operation under subpar 5.9e(5)(a).

f.The NARA ISO may authorize the escort or hand carrying of classified information outside the United States and its territories upon certification by the requestor that:

(1) the information is not present at the destination;

(2) the information is needed urgently for the stated official purpose; and

(3) there is a specific reason that the information could not be transmitted to the destination by other approved means in sufficient time for the stated purpose.

5.10 Transmission by Other Agency Couriers

a. If cleared staff or contractor from another agency needs to take copies of classified documents with him or her, he or she must produce a valid courier badge, or memo on official letterhead from their agency, granting authority to courier classified information at the classification level of the documents. If the other agency courier has a lockable courier pouch or briefcase, NARA staff will prepare the initial wrapping (inner envelope or container), place the wrapped documents in the pouch or briefcase (which serves as the outer container), and have the courier secure the lock. If the courier does not have a

lockable container, NARA staff will prepare both the inner and outer containers, ensuring that the documents are double-wrapped. The other agency courier must sign for the package contents on NA Form 2011, Classified Document Control Record, or other NARA-produced receipt, in accordance with par 5.4 of this handbook.

b. If the other agency individual needs copies of classified documents, but does not have a courier badge or memo, the documents are left with the NARA sponsor for later transmission to the individual's agency. The NARA sponsor must obtain a valid mailing address, wrap and dispatch the information, as appropriate, in accordance with par 5.4 of this handbook.

5.11 Dispatch to Foreign Governments

Before transmitting U.S. classified information to any foreign government, the equity holder must determine that the disclosure is consistent with the foreign policy of the United States toward the receiving government. Disclosure of classified information to foreign governments is not permitted when prohibited by law, Presidential orders, directives, international agreements, or other U.S. policy.

a. Transmission of classified mail to foreign countries requires the advance approval of the NARA ISO and the senior security official of the equity holding agency.

b. The preparation, including classification markings and method of transmission of documents, is the same as prescribed in this chapter for all other classified information of the same classification level. Normally, classified information that has been approved for release or transmittal to a foreign government takes place between designated government representatives at the receiving country's embassy in the United States.

c. The requirements in this paragraph are not applicable to NATO information, which must be safeguarded in compliance with USSAN Instructions.

5.12 Hand Carrying Controlled Access and COMSEC Information

Procedures for hand carrying controlled access and COMSEC classified information are virtually the same as described in par. 5.9 for other categories of information; however, for specific guidance consult your ISPM or the NARA ISO, and the following governing directives:

a. DOE Order 471.6, Information Security, for RD/FRD information;

b. ICD 703, Protection of Classified National Intelligence Including Sensitive Compartmented Information, for SCI;

c. Governing directives of the SAP originator, this handbook, 10 U.S.C. 119, 50 U.S.C. 2426, and the NISPOM, as applicable, for SAP information;

d. USSAN 1-07 for NATO information; and

e. NSA/CSS Policy Manual 3-16 for COMSEC material.

Chapter 6

DECLASSIFICATION AND RECLASSIFICATION

6.1 Declassification

Information can be declassified once it has been reviewed and determined to meet standards under E.O. 13526. However, when the public interest outweighs the need to protect information, it may be declassified through mandatory review, the FOIA, and by consulting with equity holders. The Archivist of the United States, may consult with heads of other agencies that have equity in the information who determine whether the public interest in disclosure outweighs continued protection, and any potential damage to national security that may be reasonably expected. In addition, if the Director of ISOO determines that information is classified in violation of E.O. 13526, the originating agency is required to declassify the information. The governing authorities for declassification policy for NARA are E.O. 13526, 36 CFR Part 1260 and this handbook. Detailed declassification procedures for Federal records, Presidential records, Nixon Presidential materials, and donated historical materials are outlined in 36 CFR Part 1260 and further supplemented in local NARA SOPs.

6.2 Declassification Authority and Use of Markings

Information in the legal custody of NARA must be declassified as stated in 36 CFR Part 1260, and marked as described in 32 CFR Part 2001.25 and in the following paragraphs. Only the Archivist of the United States or the Deputy Archivist, in consultation with the Director of ISOO, may authorize the use of other declassification markings.

a. Authority to Mark:

(1) NARA personnel authorized by the Archivist, the Director, National Declassification Center (ANDC), or the Office of Presi[illegible] [Return to TOC]
review and declassify information under E.O. 13526 an[illegible]
may place declassification markings on documents and material containing information that is declassified.

(2) Employees not personally authorized to declassify information may, under the supervision of a staff member described in subpar 6.4a(1), mark documents previously determined to be declassified.

b. Marking Declassified Records. Apply declassification markings uniformly and conspicuously so there is no doubt regarding the declassified status of the information and the identity of the person authorizing the declassification. Update the classification status in the appropriate databases, e.g., ADRRES, Holdings Management System (HMS), etc., and apply the following markings to records, or copies of records, regardless of media:

(1) the word, “Declassified”;

(2) the identity of the declassification authority, by name and position, or by personal identifier (such as initials), or the title and date of the declassification guide;

(3) a declassification project number, if applicable, the date of declassification; and

(4) a straight line or "X" through the overall classification markings appearing on the cover page or first page of the document. A couple of examples might appear as:

~~SECRET~~
Declassified by David J. Smith
Supervisory Archivist, NARA, August 17, 2012

or

~~SECRET~~
Declassified by: DJS
Project #_____, ANDC, August 17, 2012

c. Take the following specific actions to mark a document that is declassified:

(1) Conspicuously place the declassification marking on the first page of the document. Cancel all earlier classification markings on each document, or the part of the document being reproduced, by lining through them. Ensure the markings are not so obscure as to be unreadable. Use only pens with archival ink, as specified by the Preservation Programs Division (RX), when marking original documents. Use rubber stamps applied to original documents with inked stamp pads available through, or as specified by RX. When there are a large number of pages in a discrete document, cancel at least the current classification markings on the front cover, if any, or on the first page. Cancel classification markings on subsequent pages if there is a likelihood that they might become separated from the front cover or first page.

(2) When the volume of classified information is so large that each item cannot be marked without unduly interfering with operations, a declassification label may be attached to the upper flap of the archival storage container. Each label must state the authority for the declassification, the record group number, the entry number or title, and the container number. When single documents are permanently withdrawn from a storage container, withdrawn for public exhibit, or withdrawn for reproduction purposes, they or the reproduced copies must be properly marked to show declassification.

d. Information Declassified Pursuant to Sections 3.4 or 3.5 of E.O. 13526:

(1) Record items being removed from containers which have been systematically reviewed under the systematic declassification review provisions of section 3.4 of E.O. 13526, and the regulations, directives, guidelines, or instructions of the originating or successor agency which authorized NARA to take declassification action, and which bear declassification labels, may be individually marked declassified as follows:

DECLASSIFIED
E.O. 13526, Sec. 3.4
_____

(2) Enter the case or project number, or any other particular authority appearing on the declassification label, on the blank line. Place any agency correspondence, or other record of declassification authorization, in the case or project folder.

(3) Upon receiving instructions from originating or successor agencies authorizing NARA to declassify their information, use a stamp as shown in the following example to mark individual items containing information declassified under the mandatory review provisions (section 3.5) of E.O. 13526:

DECLASSIFIED
E.O. 13526, Sec. 3.5
_____

By _____, NARA, Date _____

or

DECLASSIFIED
E.O. 13526, Sec. 3.5
_____

Project #_____, ANDC, August 17, 2012

(4) The pertinent agency guideline or instruction that authorizes the declassification must appear in the blank on the third line. This instruction may also include a project or case file number.

(5) To complete the stamp mark's final line, NARA staff members authorizing the declassification marking enter their name, or initials, and the date the marking is applied. If another staff member applies the declassification marking under the supervision of a NARA declassification authorizing official, they enter the authorizer's name on the final line and place their own initials and date after the authorizer's name.

e. Information Declassified Under Other Authorities:

(1) Use a stamp as shown in the following example to mark individual items that are declassified on a basis other than E.O. 13526 (e.g., the Atomic Energy Act of 1954, as amended, regarding RD/FRD, and E.O. 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems):

DECLASSIFIED
Authority _____
By _____, ANDC (or) NARA, Date _____

(2) The agency instruction authorizing the declassification and the date of the instruction or the declassification project number must be cited on the authority line.

(3) To complete the final line of the stamp mark, enter the name or initials of the NARA staff member authorizing the declassification marking, followed by the initials of the person doing the marking (if different from the authorizing person), and enter the date when the marking is applied.

f.Special Marking Procedures for Reproductions. When reproducing large quantities of declassified documents, there is an alternative procedure for marking the documents:

(1) An acceptable alternative to marking original documents, or their reproductions, is to place a slip of paper with the declassification authority applicable to the documents being reproduced on the reproduction equipment plate, causing it to appear on each page reproduced. This procedure is recommended for reproducing many documents from the same file. The classification marking itself should be canceled on the reproduction as described in subpar 6.4c.

(2) If the quantity of records reproduced is also substantial, cancellation of the classification markings may be waived by the custodial unit's ISPM as long as the declassification authority is reproduced on each page. This should be done only upon a determination that the:

(a) workload in the unit precludes cancellation of the classification markings on the number of documents involved; or

(b) appearance of both classification and declassification markings on the reproductions will not lead to any misunderstandings as to their current security classification status (i.e., that they are declassified).

g. Marking Non-Paper Items. Marking declassifications and authorities on reproduced photograph negatives, motion picture film, and microfiche presents special problems. The film jacket, envelope or box, containing non-paper items that were reproduced for a researcher, must carry the proper declassification marking or label. Any classification marking that can be read without a reader must be canceled. A leader bearing the

declassification marking should be spliced to any roll microfilm or motion pictures reproduced.

6.3 Challenges to Classification

a. If holders of classified information at NARA, in good faith, believe that the classification status of information is improper, they are encouraged and expected to submit a classification challenge through the NARA ISO to the equity holding agency, in accordance with section 1.8 of E.O.13526. Challenges must be in writing, but may be as simple as a question as to why the information is or is not classified, or is classified at a certain level. Challenges containing sensitive or classified information may be submitted to the NARA ISO by secure fax at 301-713-6287.

b. The ISO reviews each challenge and, if it appears to be valid, the ISO submits the challenge to the equity holding agency. The equity holder should provide a written response within 60 days. If they are unable to respond within 60 days, they must acknowledge the challenge in writing, and provide an alternate date by which they intend to respond. The acknowledgment includes a statement that if no response is received within 120 days, the challenger has the right to forward the challenge (through the ISO) to the Interagency Security Classification Appeals Panel (ISCAP) for a decision. Include the challenger's right to appeal to the ISCAP in the response to challenges that an agency has denied.

c. No retribution or unfavorable personnel action may be taken against any NARA employee who makes classification challenges in good faith.

6.4 Reclassification

This section outlines the procedures that must be followed upon identification of previously classified information that may have been designated unclassified with or without proper authority. Please refer to 32 CFR Part 2001.13 and 36 CFR Parts 1260.80 and 82. NARA must balance the need to ensure that archival records are both available to researchers while at the same time addressing legitimate national security concerns.

a. Reclassification of information previously declassified and released under proper authority:

(1) Records in the physical and legal custody of NARA that have been made available to the public following declassification and release to the public under proper authority in accordance with E.O. 13526 (or predecessor orders) may be considered for reclassification at the request of an agency. The agency head must submit a written determination on a document-by-document basis notifying the Archivist that the reclassification of the information is necessary in the interest of national security. The information must be reasonably recoverable without bringing undue attention to the information and meet all other conditions of section 1.7(c) of E.O. 13526, and 32 CFR Part 2001.13(b).

(2) Reclassification requires notification to the Archivist and approval by the Director of ISOO. The Archivist will suspend public access pending approval or disapproval of the reclassification request. The decision of the Director of ISOO may be appealed by the Archivist or the agency head to the President through the National Security Advisor. Public access will remain suspended until a decision is made on the appeal.

(3) If the request is approved, brief current security clearance holders in possession of the reclassified information about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. To the extent possible, brief non-clearance holders who may have had access to the reclassified information on their obligation to not disclose it, and request that they sign an NA Form 3056, Inadvertent Disclosure Agreement.

(4) Within 30 days after reclassification of information that was previously released under proper authority, the requesting agency head must report the details and recovery actions specified in 32 CFR Parts 2001.13b(1) & (3) to the National Security Advisor and the Director of ISOO.

b. Reclassification of information previously declassified without proper authority:

(1) Records in NARA's physical and legal custody that have been made available to the public following declassification without proper authority, as determined by an original classification authority with jurisdiction over the information, remain classified. The original classification authority should consider whether withdrawal from public access and reclassification of the information will significantly mitigate harm to the national security, or draw undue attention to the information, and notify the Archivist in writing in accordance with 32 CFR 2001.13(a)(1). Upon notification, NARA will take administrative action to restore markings and controls, as appropriate. In cases where NARA discovers mistakenly released records due to processing errors by NARA staff, NARA will immediately notify the original classification authority for a determination and formal request, if any, to withdraw the records from public access.

(2) If the Archivist does not agree with the reclassification decision and the information is more than 25 years old, the information will be temporarily withdrawn from public access and the Archivist will appeal the agency decision to the Director of ISOO, who will make a final decision on the classification status. The decision of the Director of ISOO may be appealed by the Archivist or the agency head to the President through the National Security Advisor.

c. Information about records that have been reclassified or have had their classification restored as described in 36 CFR Parts 1260.80 and 82 will be made available through the NARA web site, Quarterly Report of Withdrawals of Previously Declassified Records.

Information will include the responsible agency, NARA location, date withdrawn, number of records, and number of pages.

d. Reclassification of White House Originated Information. Previously classified publicly available archival records may have been designated unclassified, with or without proper authority. An agency or an entity within the Executive Office of the President that solely advises and assists the President, may ask NARA to withdraw, temporarily close, review, and possibly reclassify or restore the classification of White House originated information that has been declassified and previously released. That agency or entity must follow the same procedures as a request for reclassification of executive branch information in the preceding subpars 6.4a through 6.4c, and 36 CFR Parts 1260.80 & 82.

[Return to TOC]

Chapter 7

DISPOSAL AND DESTRUCTION

7.1 General

Carry out destruction of classified information in NARA facilities in accordance with this handbook; 32 CFR Part 2001; 36 CFR Parts 1229, 1233 and 1235; or other authorities governing special categories of classified information, e.g., CNSS Instruction 4004, Destruction and Emergency Protection Procedures for COMSEC and Classified Material**,** when applicable. The disposal procedures outlined here apply to record and non-record information.

a. Records scheduled as permanent and records that have already been accessioned may only be destroyed in the special circumstances described in 36 CFR Parts 1229 and 1235.34. Classified information having permanent retention value, stored in or on media that deteriorate over time, e.g., microfilm, microfiche, disk media, carbon sheets or plates, typewriter ribbons/cartridges, etc., may be copied onto new media and retained, as the record copy if the original has deteriorated.

b. Presidential records can only be destroyed in accordance with the Presidential Records Act and NARA 1461, Disposal Guidance for Presidential Records.

c. Temporary Federal records in NARA's legal custody may only be destroyed as specified in 36 CFR Parts 1233.20. Unscheduled records must not be destroyed. After such records have been scheduled as temporary, they may be destroyed only when the authorized retention period has been reached.

d. Non-record classified information must be destroyed as soon as its intended purpose is served.

e. All classified and unclassified papers, consisting of record and non-record, usually operational, material not having permanent retention value must be shredded or placed in red and white-striped classified waste "burn" bags for destruction. Arrange for the destruction of burn bags locally through your ISPM, or at Archives I and II though the Facility and Property Management Division (BF). Mark burn bags as shown in par 7.3. Trash cans may be used only for obvious trash items such as bottles, cans, metal fasteners, tissues, etc.

7.2 Methods of Destruction

Destroy classified information only by burning, pulping, melting, chemically decomposing, pulverizing, degaussing, crosscut shredding, or mutilating to the extent that the information cannot be recognized or reconstructed. The following requirements must be satisfied when matter containing classified information is destroyed.

a. Destroy classified microforms only by burning, chemical decomposition, disintegration, or other methods approved by the ISO or cognizant ISPM.

b. Destroy classified IT systems storage media only by pulverizing, melting, degaussing, incinerating, disintegrating, or other appropriate methods approved by the NARA Information Technology Security Division (IT), in coordination with the ISO or cognizant ISPM.

c. Certain methods of destruction may require additional considerations or approvals before they are used:

(1) Destruction of paper products. Pulpers, shredders, or pulverizers (e.g., hammer mills, choppers, and hybridized disintegration equipment) should be used only for the destruction of paper products. Only paper-based products should be destroyed by pulping. Water-repellent papers or other supports, including Mylar and durable medium paper substitutes, are not sufficiently destroyed by pulping. Other methods, such as disintegration, shredding, or burning, must be used to destroy these types of papers. Paper products may be recycled only after shredding by approved methods.

(2) Destruction of high-density data documents. Classified documents in microform (e.g., microfilm, microfiche, etc.) or similar high-density data document types may be destroyed by burning, chemical decomposition, or other methods as approved by the ISO or cognizant ISPM. These types of documents may also be destroyed by using equipment designated for that purpose as referenced in par. 7.4.

(3) Tapes, diskettes, and cassettes. To ensure that memory is physically destroyed, these items must be thoroughly erased before being destroyed by pulverizing, melting, incinerating, disintegrating, or other methods as approved by the ISO or cognizant ISPM. Removable and non-removable hard disks also may be destroyed by removing the entire recording surface through sanding or applying acid.

(4) Cylinders and sound recordings. This media may be destroyed by shaving, breaking, tearing, or incinerating.

7.3. Containers

a. When burn bags or boxes are used for the collection of classified information going to central destruction facilities, such bags or boxes must be controlled to minimize the possibility of unauthorized removal of the container or the classified contents before actual destruction.

b. Each container must be marked by the office generating the classified waste to show the highest classification of information within the container, the office symbol, and the responsible individual's telephone extension number. For example:

c. When filled, staple or seal the containers in a manner that will show any tampering with the container.

d. Burn bags must weigh no more than 10 pounds. Boxes must be no more than one cubic foot, such as the Federal Records Center (FRC) box.

e. Trash cans may be used only for obvious trash items such as bottles, cans, metal fasteners, tissues, etc. Paper products may be recycled only after shredding as described in par 7.4.

7.4 Equipment

a. Only equipment listed on an NSA Evaluated Products List (EPL) is authorized for the destruction of classified information.

(1) Equipment listed on the EPL for high security crosscut shredders may be used for destruction of classified paper materials. Strip shredders are not authorized for use in destroying classified information.

(2) EPLs of approved destruction equipment for classified information maintained in other forms, including degaussers for classified media, may also be found on NSA's public web site.

b. Equipment that has been discontinued or no longer manufactured may be utilized for the destruction of classified information as long as it remains on the EPL.

c. NSA issues guidance on the methods, equipment and standards for destruction of classified information, electronic and optical media, and processing equipment components. The Committee on National Security Systems (CNSS) issues guidance on the methods, equipment and standards for destruction of COMSEC material.

d. Pulping equipment must be equipped with security screens with perforations of ¼ inch or smaller.

e. Pulverizing equipment must be outfitted with security screens that meet the following specifications:

(1) Hammer mills—the perforations must not exceed 3/16 of an inch in diameter.

(2) Choppers and hybridized disintegrators—the perforations must not exceed 3/32 of an inch in diameter.

7.5 Destruction Facilities

Classified information must be destroyed at facilities approved by the NARA ISO or by the ISPM representing the NARA activity holding the records that have been designated for destruction.

a. If classified information cannot be destroyed on-site, they must be destroyed at a NARA-approved destruction facility by a cleared individual on the same day they are removed from the on-site location.

b. Ash residue produced by burning must be examined and physically stirred or mixed to ensure that the matter is completely destroyed and no unburned matter remains. When this is not possible due to safety concerns or limitations imposed by the destruction facility, the material must be placed directly into the chute of an active incinerator.

7.6 Judicial Stays or Prohibitions

If an agency is subject to a court order prohibiting records destruction, special procedures may be required. Under such circumstances comply with guidance provided by NGC and the equity owning agency's records management officer.

7.7 Witnesses

a. The destruction of classified matter must be accomplished by individuals who have appropriate access authorization for the classification of matter to be destroyed. Except as outlined in subpar 7.7b, destruction may be accomplished by one individual; no additional witness is required.

b. Disposition of COMSEC, FGI, NATO and RD/FRD matter, and any required documentation, must be compliant with the following respective governing regulations:

(1) COMSEC in accordance with CNSSI 4004, Destruction and Emergency Protection Procedures for COMSEC and Classified Material.

(2) FGI in accordance with existing treaties or agreements and 32 CFR Part 2001.54.

(3) NATO information in accordance with USSAN Instruction 1-07.

(4) RD/FRD matter in accordance with DOE Order 471.6, Information Security.

7.8 Recordkeeping

a. Use NA Form 2011, or other appropriate form, as outlined in Chapter 5 of this handbook, to document the receipt, transmittal, and destruction of classified information. Do not create new records for the sole purpose of documenting destruction, except when mandated for the categories of information referenced in subpar 7.7b.

b. A record of dispatch is not required unless custody of the classified information is released to another cleared contractor or a government agency.

c. All records used for, or specifically created when necessary, to document the destruction of classified information must be kept for at least two years under NARA records schedule, item 254.

[Return to TOC]

Chapter 8

SECURITY EDUCATION, TRAINING AND AWARENESS

8.1 Introduction

The NARA ISO implements and oversees a security education and training program for all NARA employees. The program is designed to maintain security awareness among employees and contractors, impress upon them their security responsibilities, and prevent security incidents. The program is made up of four elements: formal training, briefings, self-evaluations, and awareness reminders. As a basic part of NARA's classified information security program, all employees holding security clearances must familiarize themselves with NARA 202 and participate in security education, training and awareness. ISPMs conduct this training for staff members under their cognizance.

8.2 Training Goals

As a result of their training, NARA employees and contractors should:

a. understand classified information security program policies and requirements, their importance to the national security, and how to apply them at work;

b. maintain continuing awareness of NARA's security environment and possible threats;

c. actively promote and support classified information security program goals; and

d. acquire the necessary knowledge to perform the security functions in which they may be involved.

8.3 Security Education

The NARA security education program consists of one-time and recurring briefing and training sessions.

a. Cleared personnel working with classified information:

(1) The ISO offers training to NARA employees who are appointed, or otherwise assume responsibilities as an ISPM or SFM. Training covers the required knowledge of the position as specified in NARA 202, subpars 202.4h and 202.4i, suggested applicable security-related professional development courses. The ISO provides continuing advice and guidance as needed, to ensure quality performance in the position.

(2) NARA employees and on-site contractors who hold an active security clearance must undergo initial training as specified in par 8.4 of this handbook and subpar 202.4j of the NARA 202 directive, attend all required

briefings, and complete at least one session of refresher training each year. ISPMs ensure that the cleared employees in their units receive the required security education and must maintain records of training offered and employee participation.

(3) NARA employees who may need to create derivatively classified documents must receive training from their ISPM on the proper application of derivative classification marking at least once every two years as required by 32 CFR Part 2001.70. Only NARA employees who have received the required training may derivatively classify documents. Employees who do not receive the required training at least once every two years will have their ability to derivatively classify documents suspended.

b. Other personnel:

NARA employees and on-site contractors not cleared for access to classified information should be included in the security education program, as outlined in NARA 202, subpar 202.4j, if they work in situations where inadvertent access to classified information might occur. Supervisors should encourage individuals in this category to attend at least one session of security-related training each year. Non-cleared staff must also understand the nature and importance of classified information and the actions they should take if they find unsecured classified information, note apparent security vulnerabilities, or have been solicited by persons without a need to know for information that is classified or otherwise not available to the public.

8.4 Briefings and Training

a. Initial training and briefing. All NARA employees and on-site contractors approved for access to classified information must complete modules 1 through 3 of the online "Safeguarding Classified Information" course as soon as possible after the individual begins employment in a sensitive position that requires the access. Module 1 must be completed prior to receiving the security clearance. Employees must also receive an SF 312 briefing and sign the SF 312, Classified Information Nondisclosure Agreement, within 15 days of notice to the supervisor that the individual's security clearance has been approved. The signed and witnessed SF 312 form must be returned to the Personnel Security Officer, along with the completion certificate for module 1 of the online training. Modules 2 and 3 must be completed within 30 days after the individual's SF 312 briefing. Additional nondisclosure agreement forms, such as those mentioned in par. 3.14, are used to brief individuals for access to controlled categories of classified information. The initial training and SF 312 briefing:

(1) advise employees of the need to protect classified information, the unfavorable effects to national security that could result from unauthorized disclosure, and their responsibility for protecting classified information;

(2) orient employees to the principles and procedures for declassifying, controlling, storing, transmitting, downgrading, marking and destroying classified information;

(3) familiarize employees with the security requirements they are expected to meet while employed at NARA;

(4) inform employees of the techniques employed by persons who attempt to obtain classified information, and their responsibility for reporting such attempts;

(5) advise personnel of the legal penalties for unauthorized release of classified information;

(6) advise employees against discussing classified information over the telephone or e-mail, or in any other way it could be compromised;

(7) inform employees of the disciplinary actions that may result from violating or disregarding NARA security policies;

(8) instruct employees that before providing access to anyone, they must determine if the recipient is properly cleared for access by a competent authority, that they need the information to perform their official duties, and that they have approved facilities to properly protect and store the information;

(9) advise employees of the obligation to report any conduct or activities they become aware of involving individuals with access to classified information, that violate conditions of access, such as:

(a) involvement in activities or sympathetic association with persons who practice or advocate the overthrow of the United States Government;

(b) criminal behavior;

(c) unexplained affluence or excessive indebtedness; or

(d) unwillingness to comply with rules and regulations or security requirements.

(10) advise employees when involved in outside activities as members of professional, commercial, scholarly and advocacy organizations, or in social settings, to not reveal classified information or information about their job or work facility that may not be publicly known and could be valuable to persons wishing to do harm to NARA or its personnel;

(11) instruct employees to immediately report any loss or possible compromise of classified information as specified in Chapter 9 of this handbook; and

(12) instruct employees, as applicable, on the proper application of derivative classification markings. See Chapter 2 and subpar 8.3a(3) in this chapter for specific guidance.

b. Refresher Training. The ISO arranges for periodic briefings, training sessions, other formal presentations, and online courses that reinforce the policies, principles and procedures covered in the initial training and briefing, along with this handbook. ISPMs provide this training locally. Refresher training must also address local issues and concerns identified during annual self-evaluations. All security clearance holders, having already completed modules 1 through 3 of the online "Safeguarding Classified Information" course, will also take online refresher training at least annually, or more often as directed by their ISPM or the ISO.

c. Other Training. Staff who work in secure facilities, or who are assigned additional security responsibilities, must complete modules 4 through 6 of the online "Safeguarding Classified Information" course, depending on their security role as described in the NARA 202 directive. The ISO and ISPMs provide continuing security education to enhance individual security performance at NARA. They may supplement periodic briefings and refresher training with other information and promotional efforts to help personnel maintain an appropriate level of security awareness, and use other items, e.g., posters, newsletters, flyers, postings on the web, etc., to complement formal training when they are the most effective means of achieving program goals. Do not circulate directives or informational material on a "read and initial" basis as the sole means of fulfilling any of the specific requirements of this chapter.

d. Foreign Travel Briefings. All Government staff and contractors employed at NARA who hold a security clearance and plan to travel overseas, are obligated to report their personal and official foreign travel on NA Form 3057, Notification of Foreign Travel, prior to departure.

(1) Individuals should go to the Foreign Travel Briefings section of the Safety, Security & Emergency page on NARA@work and follow the links to read the following information:

(a) NARA Defensive Travel Briefing;

(b) Current Travel Warnings and Advisories; and

(c) Foreign Country Sanctions. If your destination country is subject to a current travel warning or sanction, notify the ISO immediately; you may not be able to travel unless you comply with the posted requirements.

(2) Complete the notification and acknowledgement sections (page 1) of the NA 3057 and submit the form to your supervisor.

(3) Upon return, complete the Foreign Travel Debriefing portion (page 2) of the NA 3057 to describe any incident which indicated a security threat.

(4) Once both pages of the NA 3057 have been completed, supervisors will forward the form to the NARA Personnel Security Officer for inclusion in

the individual's personnel security clearance file, under file no. 312-1 of the NARA records schedule.

e. Termination Briefings:

(1) The unit's ISPM or the NARA Personnel Security Officer must debrief all cleared employees, including those with access to SCI and SAP information, Restricted Data and Formerly Restricted Data, and complete the appropriate security termination agreement when:

(a) reassigned to a non-sensitive position that does not require access to classified information;

(b) they will be absent from NARA for 120 calendar days or more;

(c) they leave NARA employment; or

(d) access to classified information is revoked.

(2) Send termination agreements to the NARA Personnel Security Officer (BX) who retains the form in accordance with the NARA records schedule, item 315.

(3) Report the refusal to sign a security termination agreement to the Personnel Security Officer (BX). See NARA 273, Collateral Security Clearances for more information.

8.5 Awareness

Security awareness is everyone's responsibility. The NARA ISO and ISPMs at each NARA component must establish a continuing security awareness program that provides frequent exposure to security awareness material. A continuing program may include briefings, audiovisual presentations (e.g., video tapes, films, and slide/tape programs), or printed material (e.g., posters, memorandums, pamphlets, fliers). Use current information and materials and design programs to meet the particular needs of the component. The awareness program should emphasize and reinforce the points contained in subpar 8.4a.

8.6 Program Oversight

NARA offices provide additional security training to all their personnel through their ISPMs, who must evaluate the effectiveness of the training during annual self-inspections. Evaluations must assess the quality and relevance of the training, as well as adequate staff participation. ISPMs must maintain records of training and employee participation in accordance with NARA records schedule, item 212-1.

8.7 Inspections

Annual self-inspections (see NARA 202 subpars 202.4h(16) and 202.4i(11)) are a test of the effectiveness of the classified information security program and provide evidence of training

needs. ISPMs and SFMs must use self-inspections to review local compliance with NARA policies and procedures for the protection of both collateral and categories of classified information. Use only self-inspection checklists provided each year by the ISO to gauge current security compliance in your area of responsibility. Additionally, ISPMs and SFMs must:

a. test secure facility alarms every six months and keep records of the test results;

b. recertify classified reproduction equipment to make sure they are working properly and annotate the NA Form 2007 accordingly;

c. maintain all documentation in the secure facility management folder (ISPMs maintain their completed self-inspection checklists under NARA records schedule, item 263-2); and

d. submit copies of self-inspection results to the ISO upon completion.

[Return to TOC]

Chapter 9

SECURITY INCIDENTS AND REPORTING

9.1 Overview

The impact from the loss or compromise of classified information may cause grave damage to the national security and subject the individual responsible for the disclosure to administrative and criminal penalties. It is important that security incidents be identified and reported to the appropriate officials in order to achieve the most expedient and complete resolution of the matter. Depending on the nature of the incident, the ISO may additionally consult with OIG or NGC. Incidents of actual or suspected compromise of classified information must be investigated and reported in accordance with this handbook.

9.2 Discovery and Notification

Anyone who observes information requiring protection not being properly safeguarded, suspects a loss or compromise of information has occurred, or observes other circumstances that may result in a loss of control of classified information, must:

a. For non-electronic records, immediately report the circumstances to his or her immediate supervisor and to the local ISPM. Supervisory personnel must pass all such reports to their office executive or staff director, as appropriate, without delay. ISPMs must notify the ISO within 24 hours of occurrence. If the supervisor or ISPM are unavailable or believed responsible for the loss of control, notify the next level supervisor and the ISO directly.

b. For IT systems or electronic media, immediately contact the Information Technology (IT) Security office to initiate containment and keep the information from spreading. This initial report should be made by telephone, but should be followed up with a written notification within 48 hours. Notification of such incidents must also be made to the ISPM and the ISO. All processing may be ordered to stop on the system until it is determined if a security incident or violation exists, and the extent of the problem.

c. Make every effort to restore control of the information or materials that may have been compromised pending assumption of initial responsibility for action by the ISPM or IT Security.

9.3 Inadvertent Disclosure

An individual without the appropriate security clearance, who inadvertently gains access to classified information, must sign an NA Form 3056, Inadvertent Disclosure Agreement. The ISPM:

a. briefs the individual on the contents of the Inadvertent Disclosure Agreement (IDA) and has the individual sign the agreement;

b. determines if the information has been disclosed to anyone else;

c. impresses upon the individual the need to protect the information, and to never divulge it under penalty of law; and

d. notes in the written report (par. 9.8) that the IDA was administered, and attaches a signed copy to the report.

9.4 Unauthorized Disclosure to the Public

Report any appearances of classified information in the public media or in the control of an unauthorized individual to ISOO. As outlined in 32 CFR Part 2001.36, anyone who becomes aware of organizations or individuals who possess potentially classified information outside of government control must contact ISOO for guidance and assistance. Refer inquiries from the media regarding a security incident, or the subject matter of the incident, to Public and Media Communications (SCM). Do not make any statement or comment that would confirm or deny the accuracy or verify the classified status of the information; discuss only with appropriate NARA officials (i.e., ISOO, SCM, OIG, NGC and BX).

9.5 Security Incident Risks with IT Systems

Use of the internet and e-mail has increased the number of security incidents involving accidental disclosure of classified information. This may occur when individuals download a seemingly unclassified file from a classified system, and copy it to an unclassified system or transmit it via e-mail without first verifying that the information is indeed unclassified. Immediately report the discovery of classified information in an unclassified system as indicated in subpar 9.2b to offset the potential for interception and compromise of the information. See NARA 804 for further guidance.

9.6 Preliminary Inquiry Process

When an ISPM receives a report, or otherwise becomes aware of a loss, suspected loss, or compromise of classified information, or other incident of security concern, he or she must initiate the following sequence of actions:

a. take custody of, and properly secure, any materials involved in the incident;

b. gather the basic facts (e.g., description and classification level of the information involved, likelihood of compromise, and a summary of events surrounding the discovery); and

c. notify the ISO within 24 hours of occurrence by the fastest means available. When instructed to do so by the ISO:

(1) initiate a preliminary inquiry to uncover the circumstances surrounding the reported incident, characterize the incident and establish findings;

(2) administer the IDA (NA Form 3056) to individuals who had access to classified information, but were not cleared for access to the information; and

(3) document the results of the preliminary inquiry in a written report. See par. 9.8.

9.7 Conducting a Preliminary Inquiry

After gathering all relevant information and researching applicable NARA policies, the ISPM evaluates the nature and seriousness of the incident and establishes whether classified information was compromised.

a. The preliminary inquiry must focus on answering the following questions:

(1) When, where and how did the incident occur? What happened?

(2) Was any information compromised?

(3) What specific information or materials, if any, were involved and the level of classification of the information?

(4) What persons, situations, or conditions caused or contributed to the incident?

b. Every preliminary inquiry includes a characterization of the seriousness or nature of the incident and establishes the likelihood of compromise of classified information. A minimum of two conclusions are required from the inquiry:

(1) a clear statement that a violation did or did not occur and, if it did, who committed it; and

(2) the probability of compromise – was it likely or not?

c. If, at any time, a crime is suspected or uncovered, stop the preliminary inquiry and contact the ISO, who will notify the OIG and NGC. If warranted, the OIG may assume the investigation.

d. Formal definitions for the terms used to characterize incidents are contained in the glossary, but in practical terms, they may be summarized as:

(1) a security violation is a failure to follow requirements of executive orders, laws or regulations resulting in, or holding a high probability of, the compromise of classified information;

(2) a security infraction is a failure to follow routine, technical procedures such as applying proper classification markings, showing proper declassification authority, and other actions less serious than a security violation, and that

did not, or likely did not cause, the compromise of classified information; and

(3) a practice dangerous to security is an action, such as writing down and carrying security container combinations, not properly setting a combination lock after securing an area, and other actions that did not, or hold little or no probability of causing the compromise of classified information.

e. If a compromise was likely, the responsible NARA office, or the ISO after consulting the SAO, notifies the agency or agencies that originated the information so that a damage assessment can be done and measures taken to negate or minimize any negative effect.

f. Findings must be supported by evidence, testimony (interviews), and documented in the report and must be characterized as a violation, infraction or practice dangerous to security. If classified information was involved, a statement that the classified information was, or was not, accounted for and a recommendation for a damage assessment, if compromise was likely, must be made.

g. In cases of apparent disclosure of classified information to unauthorized individuals, including the public or media, the preliminary inquiry must include the following additional questions to determine if a leak investigation is warranted:

(1) What is the date and citation of the article disclosing the information?

(2) What specific statements in the article are considered related to the information in question, and was the information properly classified?

(3) What is the extent of dissemination?

(4) Have portions of, or background data on, the information been published in an open source?

(5) Is the disclosed information accurate?

9.8 Written Report

a. Upon completion of the preliminary inquiry, the ISPM submits a completed NA 6067, Classified Information Security Incident Report (IR), to the ISO. The IR must be completed as generally described in subpar 9.6c and submitted as soon as possible after an incident is reported. The report must contain the facts and circumstances relating to the incident, including time, date, place and the identity of persons or classified information involved. In preparing the report, ISPMs must address each question raised in the previous par. 9.7 and:

(1) keep incident reports unclassified; however, if this is not possible, derivatively classify, mark, and protect according to content;

(2) handle all incident reports as Privacy Act information, exercising caution to ensure strict confidentiality. Disclosing details regarding an incident to an individual outside the investigative chain can compromise an investigation or unfairly affect the reputation of anyone involved. Inquiry and investigation reports are exempt from public release under Federal confidentiality statutes and FOIA exemption (b)(7);

(3) take corrective actions that would aid in precluding the incident from recurring, and note them in the inquiry report, such as:

(a) retraining individuals involved, when necessary, to achieve understanding of the requirement;

(b) instituting policy or procedural changes to assure that the necessary guidelines are in place to address the issues and preclude recurrence;

(c) eliminating conditions that did or could cause or contribute to the incident (e.g., covering windows during classified processing; keeping a STE card in a different security container; and

(4) make recommendations to the ISO based on the inquiry's findings:

(a) If the ISPM believes the incident has been sufficiently vetted in the inquiry process and has been resolved, he or she should recommend closure.

(b) If the issue involves another NARA office or outside agency and cannot be resolved without their involvement, the ISPM should recommend referral to that office or agency.

(c) If after exercising all due diligence to resolve the issue, the ISPM believes further effort is necessary but beyond the scope of his or her authority or ability to act, he or she should recommend referral to the ISO for further investigation. The ISO, OIG, or other qualified individual appointed by the Senior Agency Official (SAO) may then conduct a formal investigation. The preliminary inquiry report becomes part of any subsequent investigation.

b. Based on review of the inquiry, the ISO makes the following determinations:

(1) If the ISO determines that the issue can be resolved without further investigative efforts, recommendations for disciplinary actions may be added according to par. 9.9, he or she forwards the case to the SAO for endorsement and closure, then to the responsible NARA office executive for consideration of the recommended sanctions.

(2) If the ISO determines that additional investigation is required, the procedures of subpar 9.8a(4)(c) apply.

9.9 Administrative Sanctions and Closure

a. NARA employees, volunteers, interns, contractors, licensees, and grantees are subject to sanctions, also referred to as disciplinary actions, in cases cited in section 5.5 of E.O. 13526, or if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons or organizations, information properly protected under the provisions of NARA 202;

(2) knowingly and willfully violate any provision of NARA 202; or

(3) fail to report the possible loss or compromise of classified information according to the procedures of par. 9.2.

b. Individuals who commit security violations, infractions or practices dangerous to security may be subject to sanctions under the NARA Penalty Guide (Personnel 300, Appendix 752A) that may include, but are not limited to warning notices, reprimands, termination of declassification authority, loss of clearance, denial of access to classified information, suspension without pay, or removal. The sanction must fit the offense. The ISO recommends appropriate sanctions for security incidents involving classified information as outlined in the following paragraphs.

c. When the results of an inquiry confirm a finding of a security violation, infraction, or practice dangerous to security, the ISO may recommend sanctions to the SAO. When sanctions are recommended, the report goes to the responsible NARA office executive for implementation. Appropriate disciplinary actions as outlined above and in keeping with the NARA Penalty Guide must be seriously considered by the responsible office executive as a deterrent to ensure a similar incident does not recur. When disciplinary action is contemplated against an individual, NGC and Office of Human Capital (H) must be consulted.

d. The responsible office executive shall notify the SAO whether the recommended sanctions were, or were not taken, and if not, what actions were taken to ensure no recurrence.

e. The ISO maintains investigative reports and other inquiry-related information, to include corrective actions, for five years from the date of the report in accordance with NARA records schedule, item 314. These files are periodically reviewed for trends or patterns that may be used in security training or inspections. Details of any disciplinary actions are maintained separately for privacy reasons.

9.10 Other Notification Requirements

a. The ISO reports violations of E.O. 13526, or implementing directives, to the Director, Information Security Oversight Office.

b. Any action resulting in unauthorized disclosure of properly classified information that also constitutes a violation of criminal statutes by a NARA employee are reported to the OIG and NGC.

c. Whenever sanctions are administered to individuals holding a security clearance, or when individuals are found responsible for repeated security incidents, the ISO may refer the issue to the NARA Personnel Security Officer for evaluation of the individual's eligibility to retain their security clearance, in accordance with NARA Directive 273, par. 273.24.

d. When a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government or another U.S. Government agency, the responsible office or the ISO, advises the other Government agency, or the Department of State, of the circumstances and findings that affect their information or interests.

[Return to TOC]

GLOSSARY OF DEFINITIONS

Terms in this glossary are primarily derived from Executive Order 13526, and reflect definitions commonly accepted within the security community. The glossary is not all inclusive, but contains terms used in NARA 202 and other Government security references.

G.1 Access. The ability or opportunity to gain knowledge of classified information.

G.2 Access List. A listing of names used to designate those persons authorized to enter a secure facility or to have access to controlled classified documents.

G.3 Accredit or Accreditation. The act of granting authorization or recognition that a secure facility or information technology system meets and maintains suitable standards of security.

G.4 Agency. Any "executive agency," as defined in 5 U.S.C. 105; any ''military department'' as defined in 5 U.S.C. 102; and any other entity within the executive branch of the United States Government that comes into the possession of classified information.

G.5 Automatic Declassification. The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority or the expiration of a maximum time frame for duration of classification established under E. O. 13526.

G.6 Balanced Magnetic Switch. A device (magnetically operated switch), using a balanced magnetic field, designed to detect the opening of a secured door or other point of entry into a secure facility.

G.7 Classification. The act or process by which information is determined to be classified.

G.8 Classified Contract. Any contract that requires, or may require, access to classified information by a contractor, or his or her employees, in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government program or project which requires access to classified information by a contractor.

G.9 Classified Information. Information that has been determined pursuant to E.O. 13526, or any predecessor order, to require protection against unauthorized disclosure, and is marked to indicate its classified status when in documentary form.

G.10 Classification Markings. Plain and conspicuous stamps or printing affixed to an element of a page, document, or item to indicate level of classification thereof. Markings other than Top Secret, Secret, and Confidential must not be used to identify classified national security information. Such markings must be larger than the text type, except for paragraph classification, e-mail subject lines, and cables, which may be the same as text type.

G.11 Clearance. An administrative determination that an individual is eligible from a security standpoint to have access to classified information of a specific category. Clearance does not imply need to know.

G.12 Closed Storage. The storage of classified information only in GSA-approved security containers within an accredited facility where it is used, discussed, and/or electronically processed. Closed storage of electronic data requires the data to be resident on removable media, which can be removed from the processor and stored in a GSA-approved security container when not in use.

G.13 Cognizance or Cognizant. The authority, assigned responsibility or jurisdiction for security program management with respect to the protection of classified information.

G.14 Cognizant Security Authority. Agencies, or their representatives, authorized by E.O. 12829, as amended, or E.O. 13526, to: 1) establish an industrial security program for the purpose of safeguarding classified information when disclosed or released to industry; or 2) approve security implementation plans and procedures or certify secure facilities for the storage and protection of classified information for which they exercise legal authority and oversight.

G.15 Communications Security (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

G.16 Collateral Information. Classified information (Top Secret, Secret, or Confidential) that does not require additional controls and access requirements as does Sensitive Compartmented Information (SCI) or Special Access Program (SAP) information.

G.17 Compromise. The disclosure of classified information to persons not authorized access.

G.18 Contractor. Any industrial, educational, commercial, or other entity that has been granted a Facility Clearance (FCL) by a cognizant security authority.

G.19 Control:

a. The authority of the agency that originates information, or its successor in function, to regulate access to the information.

b. The application of systems, devices, or procedures that allows timely authorized use while precluding or delaying unauthorized use.

G.20 Controlled Area or Controlled Access Area. Any area to which entry is subject to restrictions or control for security reasons.

G.21 Courier. An individual appropriately cleared, briefed and authorized in writing to transport classified information.

G.22 Cover Sheet. A cover conspicuously marked to indicate that the document it covers contains classified information and used to protect classified information from visual observation by unauthorized personnel.

G.23 Covered Personnel. Any individual who has an appropriate and necessary reason for accessing classified records, as determined by the Archivist; who possesses the appropriate security clearances as verified by BX; and who is either an officer or employee of the United States Government, or a Federal contractor authorized in writing to access classified records under the authority of an officer or employee of the United States Government.

G.24 Critical Nuclear Weapon Design Information (CNWDI). Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munitions or test devices. Exceptions to this includes information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type, such as the components which DoD personnel set, maintain, operate, test or replace.

G.25 Crypto or Cryptographic. A designation or marking which identifies classified operational keying material, and which indicates that this material requires special consideration with respect to access, storage, and handling.

G.26 Custodian. An individual who has possession of or is responsible for the safeguarding or accounting for classified information.

G.27 Damage Assessment. An analysis by a subject matter expert of the extent to which an actual compromise or unauthorized disclosure of classified information would result in damage to national security.

G.28 Damage to National Security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility and provenance of that information.

G.29 Declassification. The authorized change in the status of information from classified to unclassified.

G.30 Derivative Classification. Incorporating, paraphrasing, restating, or generating classified information in new form, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

G.31 Destruction. The disposal or physical alteration of classified information by prescribed means that precludes its reconstruction or recovery.

G.32 Document. Any recorded information, regardless of the nature of the medium or the method or the circumstances of recording.

G.33 Document Control. A system of records and procedures whereby control is maintained over the origination, reproduction, transmission, receipt, and destruction of classified documents.

G.34 Double Wrap. To enclose material in an inner container and an outer container.

G.35 Downgrade. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

G.36 Escort. A cleared NARA employee who accompanies uncleared individuals or visitors within a secure facility, or a shipment of classified information to its destination.

G.37 Equity. Information: (1) originally classified by or under the control of an agency; (2) in the possession of the receiving agency in the event of transfer of function; or (3) in the possession of a successor agency for an agency that has ceased to exist.

G.38 Equity Holding Agency. Agency or organization that originally classified or has subject matter authority or expertise over the contents of a document and acts as steward for the information for access and sharing decisions.

G.39 Facility (Security) Clearance (FCL). An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

G.40 Foreign Government Information (FGI). Information that is:

a. provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both are to be held in confidence;

b. produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or

c. information received and treated as "Foreign Government Information" under the terms of a predecessor order.

G.41 Foreign National. Any individual who is not a citizen of the United States by birth or through naturalization, including resident aliens, students, refugees, and émigrés.

G.42 Formerly Restricted Data (FRD). Classified information jointly determined by the Department of Energy, or its predecessor agencies, and the Department of Defense to be (1) related primarily to the military utilization of atomic weapons and (2) protected as NSI. It is subject to the same restrictions on transmission to foreign countries and multinational defense organizations that apply to Restricted Data.

G.43 Inadvertent Disclosure. An unauthorized person has been involuntarily exposed to classified information.

G.44 Incident Report. A report of any event of security concern to NARA or to the national security.

G.45 Indoctrination. The initial security instructions/briefing given a person before granting access to classified information.

G.46 Industrial Security. That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry.

G.47 Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, is produced by or for, or is under the control of the United States Government.

G.48 Information Security (Program). The system of policies, procedures, and requirements established under the authority of E.O. 13526, for identifying, controlling, and protecting classified information from unauthorized disclosure.

G.49 Information Security Officer (ISO). A designated position within the Security Management Division (BX) under the Executive for Business Support Services (B). The incumbent is appointed by the Executive for Business Support Services, in his or her capacity as the Senior Agency Official (SAO) under section 5.4 of E.O. 13526, to administer and manage the overall classified information security program at NARA.

G.50 Information Security Program Manager (ISPM). An individual and alternate(s) appointed by the head of each NARA component maintaining classified information to act on behalf of the ISO in providing assistance, advice and training to component personnel and to implement the NARA classified information security program at their location. All references to the ISPM in NARA 202 apply equally to the alternate ISPM.

G.51 Information Technology (IT) System. An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

G.52 Intrusion Detection System (IDS). A security system consisting of sensors capable of detecting one or more types of phenomena, signal media, annunciators, energy sources, alarm assessment systems, and alarm reporting elements, including alarm communications and information display equipment.

G.53 L Access Authorization. A type of authorization granted by the Department of Energy indicating that the recipient is approved for access to Secret and Confidential Formerly Restricted Data and Confidential Restricted Data on a need to know basis.

G.54 Mandatory Declassification Review. The review for declassification of information based upon a request that meets the requirements of section 3.5 of E.O. 13526.

G.55 Marking. Stamping, printing, or tagging security classification designations on documents or material to indicate the assigned classification, changes in classification, declassification instructions, and any special limitations on the dissemination of the information.

G.56 Material. Any substance on, or in which, information is embodied.

G.57 National Security. The national defense or foreign relations of the United States.

G.58 National Security Information. See “Classified Information.”

G.59 North Atlantic Treaty Organization (NATO) Information. Information received from foreign nations participating in NATO that be protected in accordance with the designations on the information when received. Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside of NATO.

G.60 NATO Central U.S. Registry. The main receiving and control point for all NATO classified information within the United States, located at the Pentagon.

G.61 NATO Subregistry. A designated control point for receipt and control of all NATO classified information at an agency; under the oversight of the Central U.S. Registry. At NARA, these are designated control points where NATO information stored or accessioned by other agencies is managed.

G.62 NATO Control Points. Offices or individual control officers designated by the CUSR or a subregistry for the receipt, control, and internal distribution of NATO classified information.

G.63 NATO Control Officers and Alternate Control Officers. Individuals designated in writing by NARA officials as responsible for the security and handling of NATO classified information within their respective units.

G.64 Need to Know. A determination within the executive branch in accordance with directives issued pursuant to E.O. 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

G.65 Nondisclosure Agreement (NdA). An agreement between the individual being granted access and the U.S. Government legally binding the individual to properly safeguard, store, handle, transport or destroy classified information.

G.66 Open Storage. The storage of classified information on desks, shelves, in containers, etc., within a facility constructed in accordance with 32 CFR Part 2001.53 and authorized by the agency head for such storage. Open storage of electronic data allows the data to reside on the processor without use of removable media and does not require further storage in GSA-approved security containers.

G.67 Original Classification. An initial determination by an Original Classification Authority (OCA) that information requires, in the interest of the national security, protection against unauthorized disclosure.

G.68 Passing Clearances. Transmitting the certification of personnel security clearances (individual security clearances), and any controlled access authorizations held by individuals. Certification is sent directly from one agency's security office to the other. This is usually done with a Visit Authorization Letter (VAL) or through use of various Government-wide personnel security databases.

G.69 Personnel Security Clearance. An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

G.70 Portable Electronic Device (PED). A generic term for small, transportable electronic items that are equipped with the capabilities to process, store, transmit, receive, or manipulate electronic data.

G.71 Potential Compromise. An event where circumstances exist such that the compromise of classified information cannot be ruled out.

G.72 Practices Dangerous to Security. The failure of a person or persons to comply with established security practices or procedures, the nature of which cannot be characterized as falling within the parameters of a pre-defined incident type. An example of a practice dangerous to security would be an individual writing down a security container combination and keeping it in his or her wallet or purse.

G.73 Protected Distribution System (PDS). A wire line or fiber optic telecommunications system that includes adequate acoustical, electrical, electromagnetic, and physical security measures to permit its use for the transmission of unencrypted classified information.

G.74 Q Access Authorization. A type of authorization granted by the Department of Energy indicating that the recipient is approved for access to both RD and FRD information at the Top Secret, Secret, and Confidential levels on a need to know basis.

G.75 Reclassification. A determination by an appropriate authority that restores the classification of information that was declassified.

G.76 Redaction. The removal of classified information from copies of a document such that recovery of the information on the copy is not possible using any known technique or analysis.

G.77 Restricted Data (RD). All data concerning design, manufacture, or utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy, but excluding data declassified or removed from the Restricted Data category pursuant to 42 U.S.C. 2162 (section 142 of the Atomic Energy Act of 1954, as amended). (See “Critical Nuclear Weapons Design Information” and “Formerly Restricted Data”).

G.78 Safeguarding. Measures and controls prescribed to protect classified information.

G.79 Sanitize. Sanitization removes classified information from IT media or multi-function equipment (e.g., faxes, printers, copiers, scanners, etc.). Sanitizing involves the physical removal of all classified information in paper form from on or inside the equipment, and erasure or physical removal of media, memory, digital storage (hard drive), and any image-carrying carbon print cartridges, platens, drums, etc., so that data recovery using any known technique is unlikely. After the media or equipment have been properly checked and cleared of all physical and electronic classified information, they are considered to be sanitized.

G.80 Secure Facility or Area. An accredited storage or work area established to safeguard classified information, built to Federal Standard 832 for a vault, or to either 32 CFR Part 2001.53 or ICD 705 for a room, or group of rooms, where classified material may be stored, used, discussed, and/or electronically processed, and is manned, alarmed, or guarded at all times.

G.81 Secure Facility Manager (SFM). An appropriately cleared individual appointed in writing by a NARA component to manage an accredited secure facility. The SFM assists the ISPM and ISO in administering the NARA classified information security program as it relates to classified information being stored by the NARA component within the secure facility. All references to the SFM in NARA 202 apply equally to the alternate SFM.

G.82 Secure Working Area. A type of secure facility or area that is accredited only for handling, discussing or processing classified information, but where storage of classified information is not authorized.

G.83 Security Clearance. See "Personnel Security Clearance."

G.84 Security Container. A security file container, originally procured from a Federal Supply Schedule supplier that conforms to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers must be labeled "General Services Administration Approved Security Container" on the face of the top or locking drawer.

G.85 Security in Depth. A determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, intrusion detection systems, random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

G.86 Security Incident. Any unfavorable event whereby some aspect of an explicit or implied security policy or posture is violated or threatened. Used as a general reference for an event that is more appropriately characterized through investigation as a security infraction, violation, or practice dangerous to security.

G.87 Security Infraction. Any knowing, willful or negligent action contrary to the requirements of E.O. 13526, or its implementing directives that does not meet the definition of a security violation. Infractions could include such things as failure to apply proper markings, failure to show proper declassification authority, failure to properly account for or safeguard classified documents and other actions that are not violations.

G.88 Security Violation. Any knowing, willful or negligent action: (1) that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) to classify or continue the classification of information contrary to the requirements of E.O. 13526, 32 CFR Part 2001; or (3) to create or continue a Special Access Program (SAP) contrary to the requirements of E.O. 13526.

G.89 Senior Agency Official (SAO). The official designated by an agency head under section 5.4 of E.O. 13526, to direct and administer the agency's program under which information is classified, safeguarded, and declassified. At NARA, the Archivist has designated the Executive for Business Support Services (B) to act in this capacity.

G.90 Sensitive Compartmented Information (SCI). All intelligence information and material that requires special controls for restricted handling within compartmented channels and for which compartmentation is established.

G.91 Sensitive Compartmented Information Facility (SCIF). An accredited secure facility where SCI material may be stored, used, discussed, and/or electronically processed, depending on the specific authorizations indicated in the SCIF's accreditation documentation.

G.92 Special Access Program (SAP). Any program established for a specific class of classified information that imposes safeguarding or access requirements beyond those normally required for information at the same classification level.

G.93 Systematic Declassification Review. The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value.

G.94 Technical Surveillance Countermeasures (TSCM). The techniques and measures used to detect and nullify the technologies that are intended to obtain unauthorized access to classified information.

G.95 TEMPEST. A term referring to the investigation, study, and control of compromising emanations from telecommunications and IT systems equipment.

G.96 Transmission. Sending information from one place to another by electronic means (e-mail, computer file sharing, etc.), fax, radio, microwave, laser, cable, wire, or other medium. Transmission also includes physical movement involving the actual transfer of a document or other material from one authorized addressee to another.

G.97 Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

G.98 Unclassified Controlled Nuclear Information (UCNI). Certain unclassified Government information concerning nuclear material, weapons, and components whose dissemination is controlled under 42 U.S.C. 2168 (section 148 of the Atomic Energy Act of 1954, as amended), DOE Order 471.1B, Identification and Protection of Unclassified Controlled Nuclear Information.

G.99 United States and its Territories. The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the Trust Territories of the Pacific, Midway and Wake Islands.

G.100 Vault. A windowless enclosure with walls, a floor, and ceiling of reinforced concrete or steel lined construction, and typically equipped with a GSA-approved Class 5 or Class 8 vault

door, that is designed to meet the specifications required for the storage of classified information, to significantly delay penetration from forced entry, and equipped with intrusion detection system devices on openings allowing access.

National Archives and Records Administration

NARA 807
March 5, 2007

SUBJECT: Content Rules and Requirements for NARA Web Sites (Internet, Intranet, and NARA-Hosted Extranets) and Presidential Library Web Sites

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a revised policy directive – NARA 807, Content Rules and Requirements for NARA Web Sites (Internet, Intranet, and NARA-Hosted Extranets) and Presidential Library Web Sites.

Why has this directive been revised? We have revised NARA 807 to reflect current practices and updated authorities. Revisions also address changes to content management practices following launch of our redesigned public web site, Archives.gov, and the Web Program's move from NPOL to NCON.

Specific changes include:

- Coverage expanded to include Foundation staff and Foundation-funded employees
- details added to Privacy requirements
- section added for new technology, including blogs, RSS feeds, and podcasts

Canceled directives. NARA 807, dated January 28, 2004, is cancelled.

ALLEN WEINSTEIN
Archivist of the United States

NARA 807
March 5, 2007

SUBJECT: Content Rules and Requirements for NARA Web Sites (Internet, Intranet, and NARA-Hosted Extranets) and Presidential Library Web Sites

807.1 What is the purpose of this directive?
This directive provides policy and procedures on developing the content for all NARA web sites (Internet, Intranet, and NARA-hosted extranet) and Presidential library web sites. The Web Publication Guide, which remains unchanged, is a supplement to this directive. The Guide supplements this directive by defining roles and responsibilities and explaining the specific procedures for coding and updating pages.

807.2 What is the authority for this directive?
For specific information about each of these authorities, see http://www.usa.gov/webcontent/

a. Pub. L. 105-277, The Government Paperwork Elimination Act.

b. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794(d)), and The Workforce Investment Act of 1998, which included the Rehabilitation Act Amendments of 1998, enacted on August 7, 1998.

c. OMB M-00-13: Privacy Policies and Data Collection on Federal Web Sites, June 22, 2000.

d. Clinger-Cohen Act of 1996 (Pub. L. 104-106).

e. Electronic Freedom of Information Act Amendments of 1996 (Pub. L. 104-231)

f. Executive Order 13166, "Improving Access to Services for People with Limited English Proficiency," August 11, 2000.

g. E-Government Act of 2002, Public Law 107-347, and OMB Memorandum M-05-04, "Policies for Federal Agency Public Websites," December 17, 2004, addressing section 207(f) of the E-Government Act of 2002.

h. OMB Memorandum, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," M-03-22, September 26, 2003.

i. OMB Circular A-130 (Revised, Transmittal Memorandum No. 4), "Management of Federal Information Resources."

j. No Fear Act Notification and Federal Employee Anti-discrimination and Retaliation of 2002 (No Fear Act) Public Law No. 107-174, May 15, 2002.

k. Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001: Public Law 106-554, "Guidelines for Ensuring and Maximizing the Quality Objectivity, Utility, and Integrity of Information Disseminated by Federal Organizations," February 22, 2002.

l. Small Business Paperwork Relief Act (SBPRA): Public Law 107-198, October 28, 2003.

807.3 To whom and what does this policy apply?

a. This policy applies to all NARA employees, interns, volunteers, detailees, Foundation staff and Foundation-funded employees, other non-NARA staff (hereinafter referred to as "staff"), and contractors who provide content and support on NARA web sites in any way.

b. NARA has one main public web site, Presidential library web sites, web sites supporting unique initiatives such as OurDocuments.gov, and NARA content existing on web sites supported by foundations or Federal Government partners. In this directive, the term "NARA web sites" refers to all of the abovementioned sites and future NARA web sites. All sections of this directive apply to NARA web sites unless specifically exempted. NARA content also exists on web sites supported by non-profit and for-profit partners. It is recommended that these web sites follow the guidelines in this directive.

c. This policy also applies to the usability and accessibility of application interface designs (e.g., the pages our web visitors use to search our online databases and catalogs, etc.) delivered via NARA web sites.

d. This policy applies to new versions (redesign or layout or functionality, as opposed to editorial changes or improvement in graphics) of existing application interfaces.

807.4 Definitions

See the supplement, *Definitions of Terms Used in Web Program Directives*.

807.5 Responsibilities

See the related directive, NARA 808, *Content Management for NARA's Main Public Web Site and Intranet*, which further identifies the roles and functions for complying with policies and procedures in this directive (NARA 807).

807.6 Legal content requirements

a. **Privacy**

(1) All NARA public web sites must contain a link to NARA's privacy notice or a customized privacy notice.

(2) If the web site is not hosted by NARA, that third-party-hosted web site should link to its own privacy policy, and must comply with Government web privacy requirements. Contact the Web Program for more information about Government web privacy

design guidance. A link from that site to the privacy policy on Archives.gov does not automatically satisfy this requirement. A link to the privacy policy of Archives.gov is approved only if the NARA manager responsible for the third-party-hosted web site ensures that the data management technical practices of the third party match the data management practices supporting Archives.gov.

(3) There must not be any discrepancies between the way the hosting organization manages its data and the privacy policy linked from the third-party-hosted web site. (See par. 807.15).

(4) Privacy statements are required for all NARA web sites.

(a) Post or link to privacy policies that comply with NARA policy and specifically address the privacy practices of the NARA organization and server hosting the web site on the respective web site.

(b) The policy must be accurate to the data management practices of the contractor or partner hosting the web site.

(c) If the web site is hosted by a contractor or partner, the Contracting Officer's Representative (COR) or NARA representative named in the relevant contract or agreement is responsible for ensuring that the contractor or partner adheres to the privacy policy established by the party responsible for oversight of the web site.

(d) The NARA manager responsible for the web site must determine whether Privacy Impact Assessments (PIA) for each web site are required and submit it to the Office of General Counsel (NGC) for review. See Interim Guidance 1603-1, Initial Privacy Reviews and Privacy Impact Assessments for further guidance.

(e) Write and translate Privacy Act statements that describe NARA's legal authority for collecting personal data and explain how the data will be used, into a machine readable format. These statements are called "P3P" in OMB guidance.

(5) Do not use persistent cookies on NARA's web sites unless approved by the Archivist. NARA's public web site privacy policy must assure online customers that NARA does not use persistent cookies.

(6) Write privacy statements in plain language. Refer to the *NARA Style Guide* for writing tips.

(7) NARA does not analyze the navigational behavior of individuals using NARA web sites without both the knowledge of the user and OMB approval, when required. Otherwise, only analysis of aggregated data [e.g., log files] is permitted to learn the trends of navigational behavior among visitors, in general, and not specific individuals.

(8) Photos showing participants at NARA events are allowed on NARA web sites without individuals' signatures because such circumstances do not generally invoke an

expectation of personal privacy. However, regarding circumstances in which an individual may not have reasonably expected to be publicized (e.g., work in a research room), a waiver (written consent in a format provided by NGC or in e-mail from the individual depicted) permitting distribution of the image via the web must be signed by the individual shown in the photo before that photo may appear on a NARA web site. For the photo's inclusion on Archives.gov, the waiver must be sent to the Web Program.

(9) Use information provided by the customer only for the reason(s) stated at the point of collection. Contact the customer to answer a question or to clarify a comment.

(10) NARA does not sell any personal information to third parties.

(11) NARA may transfer personal information to a third party only in the following cases to:

(a) A bank or United States Department of the Treasury account that must receive payment for a transaction that the customer initiated;

(b) A company that is contracted to assist NARA with specific services, including electronic commerce or donations, and which agrees not to sell or use personal information for other purposes;

(c) Legal authorities if it is suspected that a web site user is attempting to change or otherwise damage a NARA web site, or the individual is using the web site in violation of Federal or local laws;

(d) The Foundation for the National Archives, a non-Governmental 501(c)(3) organization that supports the programs and activities of NARA, a Presidential library Foundation or support organization, or the Trust and Gift funds, when a customer uses NARA's online services to make a donation; or

(e) Congress or a court in response to a subpoena.

b. **Accessibility**

(1) NARA web sites must comply with Section 508 accessibility guidelines for design and content of web pages and training guidance provided by the General Services Administration (GSA), the Department of Education, and other Federal agencies tasked with dissemination of this guidance. See the *Web Publication Guide* on NARA@work for additional information.

(a) Exception - Presidential audio materials, in accordance with Office of Presidential libraries (NL) reference and access policies, are exempt from this accessibility requirement.

(b) Exception two - No HTML equivalent is required for PDF files in cases where the data was converted into PDF and remains accurate and accessible. The original file should be formatted upon its creation so that accurate conversion to accessible PDF is

possible. Bit maps are not accessible and therefore are not an exception. At the location of the PDF download link, a link to Adobe's free online conversion tool must be provided.

(2) Refer to the Web Program Staff or the Lifecycle Coordination staff of the Policy and Planning Staff (NPOL) any questions about accessibility of files that provide authoritative copies of NARA holdings. If the copy:

(a) appears on a web page, contact the Web Program.

(b) is provided as part of the Archival Research Catalog (ARC), contact the Lifecycle Coordination staff.

(3) All NARA web sites must provide easily located links to statements explaining NARA facility and web site accessibility, as well as contact information for comment about accessibility of the respective facility and web site(s).

c. **Copyright**

(1) A notice of copyright must be attached to any known copyrighted work that is posted on a NARA web site. Notice of copyright means a visually perceptive marking on the work that contains the symbol ©, or the word "copyright," or the abbreviation "copr.;" and the year of first publication; and the name of the owner of the copyright.

(2) Make copyright citations concise. Draft a proposed citation using an example (such as a citation used in a NARA publication or exhibit) and request review of the citation by the editors in NPAC**.**

(3) In general, content on NARA web sites are in the public domain unless copyright is indicated. However, NARA can never guarantee the copyright status on any web site content. Users of such content do so at their own risk.

(4) NARA must comply with the requests of copyright owners in citing copyright of materials used on NARA web sites, including providing a link to the copyright owner's web site if required by the owner. However, no such link should contain an endorsement.

(a) NARA's exit page is used for all such links.

(b) If the link breaks because of change or removal of the copyright owner's web site, and the copyright owner has not contacted NARA to provide the correct web page address, NARA will remove the link.

(5) NARA is not obligated to research copyright, for example, to locate a copyright owner's web site or to contact the U.S. Copyright Office on behalf of the public**.**

(6) NARA does not watermark images.

(7) Content authors follow these procedures before posting copyrighted content:

(a) Notify the Web Program, in writing, of copyrighted content proposed for distribution via Archives.gov.

(b) Provide the Web Program the source citation for the content, if a record or document is not in NARA's holdings.

(c) Obtain the original author's permission and provide the written permission signed by the author to the Web Program. (The NARA organization negotiating with the individual is responsible for obtaining the written permission).

(d) Obtain permission from the source to distribute any work authored by a member of the public (for example, a conference paper or presentation given at a NARA conference by a private individual), or owned by a non-NARA organization. This permission must be obtained before the work is posted to the web site. The work must be relevant to NARA's mission.

d. **Endorsements**

(1) Do not include on NARA's public web sites text or image content that implicitly or explicitly conveys an endorsement of any non-Federal organization or commercial product. An exception to this policy is the use of file format icons, such as the familiar "W" icon ("Word document") and the "PDF" icons, which are commonly used on web sites to clearly indicate formats available for download, for example. Any other exceptions to this policy are made by NGC on a case-by-case basis.

(2) Post an exit notice to users when they use an external link from a NARA web site to a non-NARA web site, except where permitted by memorandums of understanding between NARA and its supporting partners and foundations. This guards against perception of endorsement. An example of an exit notice is:

> "You are now leaving the National Archives web site. We have provided a link to this site because it has information that may interest you. This link is not an endorsement by the National Archives of the opinions, products, or services presented on this site, or any sites linked to it. The National Archives is not responsible for the legality or accuracy of information on this site, or for any costs incurred while using this site."

e. **Viruses** - NARA web sites must include a disclaimer stating that NARA is not liable for how files may be affected during transmission over the Internet, and that NARA's

systems are protected against viruses. Files are believed to be free of viruses when they are requested from our servers.

f. **External links** - see subpar. 807.13g.

g. **Electronic reading room** - NARA's main public web site must provide an electronic reading room to provide online access to records that have been processed and disclosed in response to a Freedom of Information Act (FOIA) request and which NARA determines have become, or are likely to be, requested again under the FOIA.

h. **Equal employment opportunity (EEO) complaint data disclosure** - NARA's main public web site must contain summary statistical data relating to EEO complaints filed by employees or applicants. Links to "NO FEAR Act" reports must be made in compliance with current OMB guidance. Obtain current guidance from the Federal Web Content Managers Toolkit, online at FirstGov.gov.

i. **NARA's main public web site -** must provide NARA's guidelines for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by NARA. The link and content should reside in an area of the web site in which the public may reasonably expect to find it. It is at http://www.archives.gov/about/info-qual.

j. **NARA's main public web site -** must include a publication schedule listing publication priorities for content posted on NARA's main public web site. It is at http://www.archives.gov/comment/web-priorities.html.

(1) If the web content schedule and priorities as listed on NARA's main public web site, within the "About Us" directory, do not include those relevant to the Presidential libraries, Presidential library web sites must provide their information to the Policy and Planning Staff (NPOL) for inclusion in this list.

(2) Base schedules on the needs of citizens as a whole and those of major customer groups, and consider current and anticipated information needs, as well as historical legacy materials.

(3) Obtain more guidance from NARA's Web Program Director and from the Federal Web Content Managers Toolkit available online at FirstGov.gov.

(4) Managers and staff responsible for NARA public web sites not hosted by NARA (other than Presidential library web sites) must send their web content publication schedules and priorities to the Policy and Planning Staff (NPOL) for inclusion in this list.

(5) Posting of this information in one place on Archives.gov ensures that visitors can easily find this information.

k. **NARA's main public web site -** must post contact information for businesses wishing to do business with NARA.

807.7 Copies of intranets and extranets

It is prohibited to make copies of intranets and extranets for any purpose other than updates, according to content update procedure, or because of potential security risks. Obtain approval from both the NPOL Web Program staff and the IT Security Staff (NHI) if there is a need to make a copy for other purposes.

807.8 Appropriate content

Content is appropriate if it meets all of the following criteria:

a. Provides information that citizens, customers, and stakeholders want, as mentioned in feedback by the public, or by local, state or Federal Government organizations. Sources for such feedback may include contacts (phone, e-mail, or fax communications), surveys, and focus groups. Customer input is the greatest driver for deciding what content should be developed for the web sites and how people can mostly easily find that content;

b. Provides information that NARA needs our audience(s) to know;

c. Is directly related to NARA's mission;

d. Accurately describes NARA policy and practices;

e. Meets the requirements, where applicable, of a relevant contract or agreement with a third party;

f. Is updated as needed to maximize the quality, objectivity, use, and integrity of information services. Even content that may be relevant is not suitable for NARA's web sites if it is not maintained or periodically reviewed and updated, as needed, by content authors for accuracy. Outdated or inaccurate content may be removed at any time;

g. Is a professionally-designed web version of an approved communications product, such as a brochure, pamphlet, CD, poster, or other product intended to convey information to NARA's customers regarding the agency's mission and services, or to encourage interest of prospective audiences;

h. Supports a Federal regulation, law, directive, or Executive order;

i. Is approved by OMB as an information collection if any web forms meet the threshold of at least 10 people (See NARA 108, Information Collection, to get procedures on developing information collections);

j. Does not introduce services or discuss program initiatives before NARA supervisors or upper management, as appropriate, have determined program direction;

k. Does not contradict or cause confusion relative to other information published on NARA web sites or in written existing internal policy directives; and

l. Does not contain NARA policy, unless it has been approved through NARA's directives process as described in NARA 111, NARA Directives.

807.9 Non-English web content

a. Materials expressed in human-readable languages other than English may be published on NARA web sites if:

(1) The content is appropriate for dissemination online, meaning that it is information that NARA needs to communicate to the particular audience, or the audience needs the information as indicated by written or verbal feedback, surveys, or may be inferred by demographic data;

(2) The content requires no additional resources for translation or the resources are available for professional-quality translation and revision;

(3) NARA owns the content rights or the material is in the public domain; and

(4) The program manager responsible for the content is confident that the translation is accurate.

b. If translated material is produced by a contractor, the responsible Contracting Officer's Representative (COR) is responsible for ensuring, before acceptance of the deliverable, that the non-English language content is accurate.

c. Any non-English language content for which the accuracy of the translation can not be verified, is deemed to be inaccurately translated, or is inappropriate will be removed from NARA's web sites, except where the content is contained within archival records presented on a NARA web site.

807.10 Style of written content

Content must be written in accordance with the *NARA Style Guide*, located on the intranet web site, in plain language, and follow current web writing trends for ease of use. Guidance on web writing and usability and training courses are available in the Web Program area of NARA's intranet web site, NARA@work.

807.11 Technical requirements

a. NARA web sites must conform to Section 508 and Level 1 World Wide Web Consortium (W3C) design standards and technical specifications. See the *Web Publication Guide* on NARA@work for additional information.

b. Register domain names of NARA-hosted web sites through the Web Program; the domains must be .gov or Fed.us domains. Presidential library web sites must have a .gov domain—however it does not have to be the primary domain used in conjunction with the web site; a .gov domain may point to the primary domain (e.g., .com, .org, .edu, or .net) owned by the respective library's partner.

c. Creators/designers must design NARA public web sites for use by major browsers (e.g, Internet Explorer, Firefox). When considering browsers to target when designing for any particular NARA web site, any browser used by fewer than five percent of the customers using that web site, or a comparable web site, need not be considered in the design requirements.

d. NARA web sites must be usable by persons who have de-activated their browser's graphics (e.g., to save download time of graphics) and script recognition features (e.g., pop up blockers to stop receiving advertisements).

e. Programming languages used to run NARA web sites or present web content must, whenever possible, be non-proprietary, meaning no design or licensing restrictions so that NARA may easily migrate and preserve the data as needed.

f. Web site file organization (architecture)

(1) Make names of domains, directories, subdirectories, and files meaningful and logical respective to the content contained therein. Do not use unfamiliar abbreviations (not found in a standard dictionary) for file names, but make them reasonably recognizable to the general public. The only exceptions are that the specific audience would recognize the abbreviated word or name, or that the file name reflects a code, date, or number by which the content is recognized (e.g., the ARC code of a digital image, or a published report's date).

(2) Make domain, directory, and file names as short as possible and retain meaning so that the URL length is as short as possible and meaningful. For additional guidance, see *File and Directory Naming Conventions* in the Web Program section on NARA@work.

(3) The Web Program is responsible for assessing and establishing web site file architecture for NARA-hosted web sites.

g. Content authors must keep metadata current and relevant to the content. Metadata must comply with both the Dublin Core and current guidance issued by the W3C.

h. "Session" cookies, which support web-to-database transactions and client/server transfer of files over the Internet, may be used. However, do not use "persistent" cookies (which are downloaded onto the user's computer and often remain there, and most often are used to track the user's navigational behavior online) without approval from the Archivist.

i. All NARA web sites must comply with security controls and requirements stipulated by The Office of Information Services (NH). Contact NH for more information.

j. NARA's web statistics standard measurement is "visitors," - the number of instances in which visitors come to our web sites and explore our services. Do not report "unique" visits (the number of individuals) or "hits" (which is an inaccurate count of volume of visits) that are also offered in the WebTrends reports. See the supplement, *Definitions of Terms Used in Web Program Directives*.

807.12 Look/feel and functional design requirements

a. The look and feel of NARA web sites must support the following:

(1) Clear branding or identification of NARA as owner of the web site. The Web Program, web design contractor, and if appropriate, NPOL, NGC, and program offices evaluate, on a case-by-case basis, clarity of web site branding.

(2) Use of colors that view comparably across current, major browsers.

(3) Attractive, professional appearance.

(4) Standardized design within web sites (e.g., high-level navigation, footers and branding). Online exhibits and web features pertaining to an event or temporary publicity need, which often require unique branding, are an exception. However, because online exhibits usually are part of a web site, the exhibit design must include a link to the home page of the web site, in addition to a link to the index page for the exhibit.

(5) Use of readable, standard fonts used by current, major browsers.

b. In addition to the legal requirements listed in par. 807.6, the home page for any NARA public web site must include the following:

(1) Information (e.g., phone number, e-mail, or an electronic comment box) telling online visitors how they can notify NARA about issues or problems about NARA web site or problems with accessibility in NARA's facilities;

(2) An e-mail link by which online customers may contact NARA;

(3) The physical address and main phone number of NARA headquarters. If a Presidential library web site, the site must include the physical address and main phone number of the respective Presidential library and a link to the home page of NARA's main public web site, Archives.gov (www.archives.gov).

(4) A customer service phone number that online customers may call for information;

(5) The FirstGov.gov web site (www.firstgov.gov)**,** as long as required by the Government; and

(6) Links to other cross-government portals or links required by law or policy, including the No FEAR Act.

c. In addition to the legal requirements listed in par. 807.6, on Archives.gov, the following links are required:

(1) Strategic plans and annual performance plans;

(2) Descriptions of the agency's organizational structure, mission, and statutory authority;

(3) Information made available under FOIA;

(4) Web site privacy policies;

(5) Summary statistical data about equal employment opportunity complaints filed with the agency and written notification of "Whistleblower" rights and protections as required by the No FEAR Act of 2002; and

(6) The agency point of contact for small businesses as required by the Small Business Paperwork Relief Act of 2002.

807.13 Content and design rules

a. **Web presence** - NARA has one main public web site (Archives.gov), Presidential library web sites, web sites supporting unique initiatives such as OurDocuments.gov and NARA content existing on web sites supported by partners or foundations. NARA's main public web site consists of one home page that links to a variety of main categories (also called main topics), located at the web site's directory level. Each main topic page on the NARA public web site follows the current, approved design for the NARA main public web site. Organization of information (information architecture) and designs will be reasonably flexible to support the NARA brand while allowing sub-brands and unique identities (for example, for NARA's fregional operations, and for exhibits) to exist within the overall NARA brand.

b. **Organization of information**

(1) Organization of information on NARA's public web sites will support navigation by customer groups, customer needs and interests, and tasks to be performed by web users. Web sites' information architectures and designs must support this approach. The overall organization of information (information architecture) and design must not be based upon bureaucratic structures, which are not intuitive to the general public.

(2) When planning and implementing the information architecture and design of NARA web sites, use customer feedback provided through written or verbal opinion, surveys, and/or usability studies, collected in compliance with OMB rules concerning public data collections (see NARA 108, Information Collection).

c. **Handling frequently asked questions**

(1) The Web Program is responsible for the content relating to processes, services, or initiatives that cross major office lines, or relating to overall presentation of NARA on the web in coordination with program offices.

(2) The content owner of the respective content answers questions relating to a process or initiative contained within a unit.

(3) NPOL Web Program staff and/or NPOL Policy staff may review answers to questions to ensure that the answer provided does not contradict other information provided elsewhere on the web site.

d. **Application interfaces**

(1) Project managers must obtain approval from NH on any web application intended for use under NARA's main Internet web site or the intranet web site. NH reviews it to ensure compliance with NARA security and architectural standards. Also obtain approval from the Web Program, who reviews it for compliance with current usability standards.

(2) For all application interfaces on NARA web sites (unless exempted), irrespective of how the web site is hosted, project managers must involve the Web Program in development of requirements for interface design and functionality, and in review of usability test plans. The application's project manager must ensure that the interface is designed according to the usability requirements. NPOL Web Program staff is responsible for providing timely and accurate input to the interface requirements and test plans, and for providing current guidance about usability applicable to the purpose and customer profile for the application. For assistance, see the supplement, *Usability Guidelines*, available on the NARA@work intranet web site. Use of the guidelines is not a substitute for directly involving the Web Program in useable design of application/web page interfaces.

(3) The Web Program reviews application interfaces, unless exempted, for usability and accessibility and approves them before being posted.

(4) Project managers and CORs responsible for assessing the work of contractors who develop application interfaces for web delivery must ensure that contractors' skill sets include knowledge about accessible and usable design for application interfaces.

(5) Application developers must not create artwork that interprets or attempts to duplicate the look and feel of established NARA brands, logos, artwork, or emblems. The application developer who needs these graphics files should contact the Web Program (NPOL) or Product Development (NWCD) staffs, as appropriate, to provide the files so that the proper coding, file formats, and approved design are used. (See 807.13i.)

(6) These requirements do not apply to the data contained within applications, such as the Archival Research Catalog (ARC), accessed via NARA web sites.

e. **Search engines**

(1) NARA's main public web sites, Presidential library web sites, and web sites pertaining to major initiatives such as OurDocuments.gov must provide a search engine to assist visitors in locating information.

(a) Display results in order of relevancy to search criteria.

(b) Make response time (performance) equivalent to industry best

practices.

(c) This requirement does not necessarily mean that all hosting entities must purchase a search engine. If NARA's search engine supporting Archives.gov provides seamless searches of other NARA web sites, returning hits that appear within the look/feel of the web site, NARA units and partners funding NARA web sites may not have to dedicate resources to search engines. The Web Program is available to discuss on a case-by-case basis.

(2) Configure search engine interfaces in support of usability and accessibility guidelines.

(3) NARA-hosted search engines must be licensed to NARA. Search engines providing search capabilities on NARA web sites hosted by third parties must either be non-proprietary software or be owned by the third party and described as such in the Memorandum of Understanding, or Memorandum of Agreement, governing the respective web site.

f. **Online exhibits**

(1) If an exhibit will be posted online, include the costs of creating online versions of exhibits when planning the budget, design, and production planning for new physical exhibits.

(2) The online version need not include all of the content of the physical exhibit. Design of complete, large scale exhibits for online delivery can be costly and can result in a product that overwhelms the user and detracts from the online audience's focus on the "gems" of the exhibit. Therefore, exhibit planners should consider production of online exhibits that provide select items from large exhibits, rather than the whole exhibit.

(3) An online exhibit is more than the act of showing a Federal record to the public, or enhancing a finding aid for online distribution and interactivity. An exhibit tells a story. A theme must unify the exhibit, and the materials included must support the theme. A citation for each item and an appropriate interpretation of the materials must be included within the exhibit.

(4) An image of a physical exhibit in a NARA building does not qualify as a web exhibit, which must allow the visitor to navigate and explore the materials offered. Such an image, however, may be suitable in a web page promoting a current exhibit, for example.

(5) Length of text in online exhibits must be appropriately short to support usability on the web.

(6) Send the Web Program written notification of review and approval by upper management in the respective office(s) that owns the exhibit. No exhibit is posted on NARA-hosted web sites until the Web Program receives the notification.

(7) When materials are scanned, photographed, or created for use in a physical exhibit or its marketing campaign, resolution appropriate for web publication must be created as well. For graphics standards, refer to NARA's digitizing standards in *Image Use Guidelines*

available on NARA@work.

(8) Follow best practices for usability when presenting enlarged images. See the *Web Publication Guide* on NARA@work for additional information.

(9) There may be limitations on including copyrighted materials in online exhibits. Coordinate with the Web Program or NGC, as appropriate, before posting such materials on a NARA web site.

g. **External links**

(1) Links to external (non-NARA) web sites are permitted with discretion, providing that for links to non-NARA web sites an exit message (see subpar. 807.6d(2)) alerts the web user that the link takes the user away from the NARA web site. The exit alert also must include a statement that NARA is not responsible for the content contained in the referred site. Web hosts providing web site services on NARA's behalf, such as online training or online stores, are exempt from the exit page requirement. Links to commercial partners are not exempt from this requirement. See 807.6d(2).

(2) NARA content authors and the Web Program should make reasonable efforts to determine if the information in a web site referenced by a link is reliable, relevant, timely, accurate, and complete.

(3) External links are intended for the convenience of NARA's web visitors in locating information relative to NARA's mission and services, such as the provision of indexes and references to Federal records, information provided by NARA's partners as documented by contracts and agreements, and sites recognized by professional associations and individuals as helpful to customers.

(4) External links are intended to support NARA's mission. They are not intended to support private or commercial organizations or businesses. Links to .org, .gov, .edu, .mil or other non-profit sites that share historical and documentary interests inherent to NARA's mission are encouraged because of their general non-commercial, public-interest nature. Links to .com, .net, and other commercial domains are acceptable if supportive of customers' needs and relevant to NARA's mission.

(5) When providing external links for the online visitor's convenience, such as lodging and accommodation web sites helpful to NARA visitors who plan to travel to a NARA facility, whenever possible NARA Internet web sites must link to relevant, reputable web portals. These portals bear the burden of providing and maintaining links; individual companies that wish to be included in such listings must be advised to contact the owner of the portal.

(6) NARA web sites must not link to external web sites that lobby or solicit the Federal Government on positions of fiscal or political nature.

(7) The Archivist and NGC must both approve links to external web sites that receive "kickback" funds or support for volume of traffic delivered on the site. They are not allowed unless approved.

(8) The number of external links provided by any NARA web site must be limited to the number that content authors can maintain. All external links must be pertinent to the respective content topic. If external links are not being maintained or are inappropriate, the content author must remove the links. If not, then the Web Program removes them.

(9) The Web Program reserves the right to review links and add or remove links on the main public web site and web sites supporting unique initiatives at any time for any reason consistent with Federal policy or NARA guidance. The Web Program will coordinate the addition or removal of links on the Presidential libraries' web sites with the Libraries.

(10) Except for partnerships, NARA does not agree to reciprocal link arrangements, when NARA must link to an external site if that site will link to NARA.

(11) Links leading to manufacturers' or vendors' web sites, that provide software that the public may download to use in accessing content, must lead directly to the software download page. While vendors' web sites often change, and linking to a high level in the web site may be more convenient for NARA content authors to maintain, this may prove a disservice to the public who may quickly become confused about the software that they need to access the NARA content. NARA content authors must be diligent in maintaining links directly to web pages that provide the software download.

h. **Redirected web addresses (URLs), from old to new, on NARA's main public web site**

(1) Following redesign of a NARA public web site, the Web Program provides redirects for

(a) the major entry points (second level pages, one click from the home page) and most-often visited pages on the previous web site, for as long as is practical and can be supported by resources hosting NARA's web servers;

(b) former URLs listed on publications or other printed products to their new URLs, for as long as is practical;

(2) The web site must provide a message alerting users to the need to change bookmarks.

i. **Logos, Brands, Emblems, and Icons**

(1) The NARA main public web site, Archives.gov, has a primary brand intended to convey the identity of the web site in general. This brand is carried throughout the web site in a uniform way to encourage visitor comfort and trust in the web site. This means that branding of, for example, secondary pages must be similar or identical to the brand presented on the home page. The National Archives Experience and the Presidential libraries' web sites, which also broadly represent NARA's interests, have their own branding and logos.

(2) The NARA main public web site, Archives.gov, has one dominant logo which appears on the top left of each page and conveys the web site's overall look and feel, identity, and character. As presented on the web site, other NARA logos, subordinate within the web page layout, may be presented, for example: the Federal Records Centers logo, and the NHPRC logo. (See NARA 105, Approval and Use of NARA Logos, for procedures on logos.)

(3) For applications, such as Access to Archival Databases (AAD), accessed through NARA's main public web site, the Web Program will provide application project managers with the header, and if needed footer, files and instructions, to be used by systems developers applying the approved design to the application.

(4) With NGC approval, use of a corporate logo or a corporate name is permissible as a means of acknowledging a donor's gift to NARA. However, the logo or name must not link to the donor's web site. Language on NARA web sites may not acknowledge or describe the business or services that a donor provides. (See par. 807.15.)

(5) Do not use emblems or icons celebrating "awards" that cannot be confirmed as legitimate, which often are marketing gimmicks intended to encourage people to go to the "award sponsor's" web site.

(6) Icons must be purchased and licensed or professionally designed, for excellent presentation on NARA web sites. The Web Program reviews icons for quality of design, technical compliance with graphics standards, and suitability within the design and placement of NARA's main public web site.

j. **Online training**

(1) The sponsoring NARA unit or program must fund the design and maintenance of online training. If online training is hosted by NARA, NH must approve it before system configuration or interface design begins. (See Application Interfaces, 807.13d.)

(2) External links to a vendor's web site that provides training on NARA's behalf is permitted. An exit page is not required.

(3) Design and use of logos on the training web site must be reviewed and approved by both the program unit responsible for the training service, by the Web Program and by other appropriate approving officials (see NARA 105, Approval and Use of NARA Logos, for approval procedures) before it is launched. (See 807.13i.)

k. **Electronic mailing lists (including services also known as "listserves" or "LISTSERVs")** - Because of the cost and complexity of planning, establishing, maintaining, and facilitating a mailing list server, any proposal that NARA host a list server must be evaluated through NARA's IT Product Plan process (see NARA 801, Review of Information Technology Investments).

l. **"Blogs" or web logs** - Blogs are for comments, advice, and/or feedback shared

between NARA customers and staff. Blogs on NARA web sites are not intended to provide a public forum for recreational, political, or personal discussion. They are intended to assist NARA in delivering its services to the public and to foster communication between NARA and its customers. In this context, blogs on NARA web sites support free speech where Federal, NARA, and local regulations governing use of the Internet apply.

(1) NGC, NPOL, and the Archivist must approve all proposals for "blogs" or web logs.

(2) Before a blog or web log, open for public participation, is posted on a NARA web site, the NARA sponsoring program manager must develop a proposal describing:

(a) The purpose, the audience, and customers' need(s);

(b) The expected benefit to NARA;

(c) Rules governing public participation;

(d) Process and resources the program unit must dedicate to support facilitation of the online conversations and maintain the blog;

(e) How the feedback/information collected will be analyzed and used; and

(f) How participants' privacy will be protected.

(3) Submit the proposal to NGC for approval. After NGC approval, submit the proposal to NPOL Policy staff and NPOL Web Program staff concurrently. Agency personnel who manage the web site are responsible for managing the contextual and structural records necessary to adequately document the blog.

(4) If NPOL approve the request, write an Information Technology Product Plan. See Interim Guidance 801-2, Review of Information Technology Investments, for procedures on development and approval of product plans. After the product plan is developed and approved according to Interim Guidance 801-2, send the package to NPOL, who forwards it to the Archivist for final approval.

(5) Approved blogs must include the following introductory information:

(a) The purpose, including a statement that the blog is not intended to be a source of official information from NARA;

(b) Rules governing participation;

(c) A privacy statement, approved by NGC; and

(d) A way to register and accept the rules governing participation.

(6) Any information appearing in a NARA blog or on a private web site supported by an employee that appears to represent NARA but is not approved by NPOL must be removed by the owner. In general, it must not be used for formal communication. Press releases, notices, guidance, video/webcasts, and instruction posted on NARA's public web sites are appropriate methods of formal communication.

(7) Participants (whether a member of the public or a NARA employee) must be required to register to participate in the activity. Anonymous participation is not permitted on NARA web sites (internet and intranet).

(8) Blogs are subject to random NGC or Office of the Inspector General (OIG) review for appropriateness or compliance with Federal or local laws or with NARA regulations at any time.

(9) Blogs must be facilitated or reviewed, if possible by the sponsoring NARA unit. (NARA might contract out or depend on a partner to perform the review.)

(10) If the blog is not maintained, it must be removed by the owner.

(11) If the blog is, or becomes, a vehicle that does not reflect the mission of NARA, or in which illegal activities are discussed, the "blog" must be removed by the owner from the NARA web site.

m. **Really Simple Syndication (RSS) feeds or Podcasts**

(1) Really Simple Syndication (RSS) feeds or podcasts may be provided from NARA web sites providing that:

(a) NARA customers have an interest in the information provided by the feed, and NARA expects to benefit from the effort required to maintain the feed, the content and files.

(b) If served from a NARA-hosted server, NH approves the technical implementation of the feed and NPOL Web Program approves the proposed content of the feed.

(c) The program office requiring the feed dedicates the resources needed to keep the content current and to maintain it so that the information is relevant, interesting, and fresh.

(d) The web page that instructs how the feed may be retrieved includes a clear statement explaining the purpose of the feed, the intended audience for the feed, and the frequency with which the feed usually will be updated.

(2) RSS feeds and podcasts that do not support the guidance above must be removed by the owner from the NARA web site providing the feed.

(3) Agency personnel who manage the web site are responsible for managing the contextual and structural records necessary to adequately document the RSS feeds.

n. **Streaming audio or video files** - includes streaming web files and use of server-side scripts. As long as streaming files are an issue for NARA's network performance, provision of this content on NARA-hosted web sites will be rare, as governed by NARA 802, Appropriate Use of NARA Office Equipment. NH reviews and approves proposed use of all streaming files proposed for hosting on NARA servers. Streaming audio or video files are the fundamental technology of webcasts. NH may outsource hosting of streaming files as necessary.

o. **Scripts and other programming** - The Web Program, working with NARA's web design contractor, produces the majority of programming used on NARA's Internet (public use**)** and intranet (staff use) web sites that are hosted by NARA. However, partners, other contractors, or staff may provide scripts or other programming for use on NARA web sites if:

(1) The Web Program assesses the script or programming and determines if it is efficient, adds value to the functionality or content of the web site, is usable and supports the respective web site's current design, and is accessible. The Web Program's evaluation of proposed server-side scripts must occur before the proposal goes to NH for evaluation.

(2) If the scripts are generated server-side, NH determines the impact on the performance of NARA's IT network. NH evaluates scripts running on NARANET systems. If the script or programming causes degradation of performance and the effect(s) cannot be mitigated in acceptable ways, or presents security risks, NH may disallow inclusion of the script in a web site hosted by NARA.

p. **Content belonging to NARA vendors or partners and posted on NARA web sites**

(1) NARA does not post and maintain information for vendors, unless in support of a contractual agreement. NPOL and NGC must review any contractual language before such information is posted on the web site.

(2) NARA may post on its intranet (NARA@work) web site vendor-supplied information that is relevant to staff, such as cafeteria menus, security tips, etc. Such content must be managed by a designated content author by agreement of the NARA Contracting Officer's Technical Representative (COTR), and must follow NARA's current design and style guidelines.

(3) Vendor-created information relative to a NARA project, available on an extranet that should be password protected, is not considered a NARA web site, for the purposes of this policy. However, if the site is hosted on a NARA contracted or hosted server, the extranet must follow NARA's Information Technology policies. Managers and COTRs must be aware of the possibility that in legal circumstances NGC or the courts may not view such extranets as "not NARA." See the 800 series of directives on NARA@work for NARA's information technology policies.

q. **Privacy notice link** - Provide a link to NARA's privacy notice on web pages that offer e-mail links that the public may use to send messages that may contain sensitive information, such as a social security number, military service number, or credit card number, as directed by the NARA's OIG.

r. **Online stores**

(1) To aid visitors in navigating NARA's web sites, no more than one online store per web site is allowed, unless exempted; visitors do not expect to navigate among stores to explore purchase options and complete online payments.

(2) Links leading to partner vendors must be accompanied by text noting that the link destination is a partner site. See 807.6d(2).

807.14 NARA support of third party web sites

a. If NARA is the designated secretariat or a member of an interagency working group, commission, board, association, or partnership, NARA may agree to provide administrative support, including a web site or web pages on an existing NARA web site, for the initiative. Staff belonging to the involved program unit(s) will serve as the content authors for the respective web content. Creation of a new, unique web site to support the entity must be funded not only for its design but for ongoing operation and maintenance.

(1) The NARA representative for the initiative must coordinate plans for web pages in support of a third party web site with NGC and the Web Program Director to ensure that all resources and policy issues are resolved before NARA accepts responsibility for the web pages or web site.

(2) NARA may spend additional resources on new designs, in support of the initiative or partnership depending upon availability of resources and of work or project schedules.

b. If hosted on NARA computers or a computer belonging to NARA's contractor(s), the web pages must comply with NARA's web policy and procedures. Contact the Web Program for guidance regarding compliance with design policy. See par. 807.11.

c. If hosted on a non-NARA server, such as a third party or partner's web server, NARA managers involved in the partnership must ensure that the web pages do not contradict NARA policy. For example, the Regulations.gov web site is a partnership in which NARA provided interface and database design support while a partner agency hosted the system, and NARA managers ensured that NARA's identity and services were presented appropriately, and that the system could be supported by NARANET architecture in the case that NARA had to assume technical support of the system.

d. If third parties design web sites and deliver them to NARA for posting either on NARA's or contractors' computers, the sites must not be delivered to:

(1) NPOL Web Program or NH for hosting and maintenance without prior planning and allocation of resources.

(2) NARA without technical documentation, transfer of all applicable licenses, transfer of all files supporting the design, and tools or systems as needed by NARA for ongoing maintenance of the web site.

e. If the web content can be included within the current design of Archives.gov and is appropriate to the web site, for reasons of economy it should be posted within the design/presentation of Archives.gov. The main page of this new content must include an explanation about NARA's support of the third party/group.

f. If the web pages reside on Archives.gov, NGC must approve a logo representing the third party before it may be included in the web page(s).

g. If it becomes evident that the NARA content author(s) has not maintained web pages hosted by NARA on behalf of a third party, the Web Program may notify the content author that if the content is not maintained, the web pages will be removed. NPOL Web Program may recommend that the sponsoring unit revisit the requirement that NARA provide web site support on behalf of the third party**.**

807.15 NARA support of employee organizations' web sites

a. NARA's public web site is not intended to support or provide access to NARA's employee organizations and associations. Such employee organizations that wish to have a presence on the World Wide Web must obtain their own design and hosting services. However, if the Web Program agrees that the cost of the web pages are within NARA's financial ability to support, they may be supported on NARA's intranet web site.

b. NARA's web sites, in accordance with this policy's guidance concerning external links, may link to NARA employee organization's web sites if such a reference is beneficial to NARA's customers, and if NPOL Web Program and the Archivist approve the link (see subpar. 807.13g). For example, a link from Archives.gov might encourage public attendance to an association-sponsored presentation, open to the public, about an archival research topic.

c. Links to employee organizations' web sites must include an exit link with a Disclaimer statement (see subpar. 807.6d(2)).

d. Links from NARA's web site to an employee organization's or association's web site may be denied if, for example, the web site critiques or lobbies the Archivist, the Presidential Administration, or Congress, or if it solicits for commercial profit, in excess of fundraising purposes.

807.16 Recognizing donors

a. Donated funds, products, or services in support of a NARA web site can be

acknowledged as an "in kind" gift. Before recognizing a donor, you must work with NGC to determine what type of recognition is appropriate. This is handled on a case-by-case basis.

b. NARA web sites must not describe the business or services that a donor provides.

c. Reciprocal links or advertising is not permitted in exchange for free services or products provided to NARA.

807.17 How are records created by this directive maintained under the NARA records schedule?

See NARA 808, Content Management for NARA's Main Public Web Site and Intranet, for records management requirements.

807.18 Frequently asked questions

a. **I have an idea for a new web page. What should I do?** You should contact your supervisor first and then, if the idea is approved, contact the Web Program by directly contacting your Web Program liaison (a list is provided on the intranet web site under "Web Program") or by sending an e-mail to webprogram@nara.gov. For additional guidance, visit the Web Program section on NARA@work.

b. **What are some examples of appropriate links?** Appropriate links include, for example, legitimate genealogy research organizations, established archival organizations, or groups that advance the understanding and use of primary sources. See subpar. 807.13g.

c. **I have a question about e-mail addresses. Whom should I contact?** If the question is about an e-mail link on the web site, contact the Web Program at webprogram@nara.gov. If the question is about e-mail addresses and how e-mail is functioning, contact the NARANET Helpdesk at IT.Help@nara.gov. If the question is about updating an e-mail in the Employee Locator, contact updates.phonebook@nara.gov.

d. **I know of a finding aid that would help customers if published on the web. How do I arrange for that?** Contact the ARC Program Staff. See also Interim Guidance 811-2, Posting Finding Aids on the NARA Web Site until ARC Implementation.

e. **I'd like to create web pages about records I work with so that people can use the web to find this information on NARA's main public web site, Archives.gov. What should I do?** Contact the staff or manager responsible for content in the area of the web site of concern. If your suggestion is approved by the program unit responsible for the data, your supervisor will determine who will spend work time planning, writing, coding and maintaining the content. If approved, contact the Web Program to discuss next steps. If the information is specific to records, the Web Program will consult NPOL's Lifecycle Coordination staff to determine the most appropriate way to deliver this information to the public, whether as a web page or through ARC, or both.

f. **What is the process for publishing web content?** If you are a content author approved to provide and maintain content on Archives.gov or NARA@work, see the publication processes outlined on NARA@work in the Web Program section. Contact the Web Program (at

webprogram@nara.gov) for additional information and training.

g. **What are NARA's graphics standards for the web?** Standards are available on the intranet web site, NARA@work, under the Information Technology category, Web Program.

h. **Who is responsible for making sure that NARA's web sites are indexed by leading search engines?** The Web Program arranges indexing of the NARA web site and contacts search engine organizations. Because search engines increasingly require payment for these services, NARA may not be able to arrange for indexing by all search engines desired.

i. **I'd like to put a form on a NARA web site. Whom should I contact?** Contact either the Web Program or NPOL to have the form reviewed for its applicability to the web site. Either will coordinate the review with NHP, which is responsible for submissions to OMB when required and for assessing the relationship between the form and the business processes it supports. The Web Program assesses the online usability of the proposed form.

j. **I am planning to demonstrate a part, or all, of Archives.gov during an official presentation. I would like to use a DVD or CD of the web site to present the demonstration. How can I get a copy?** Either create a copy or contact the Web Program at least two weeks in advance of the date needed. To submit a request to the Web Program, include 1) the highest page in the site from which the navigation of the demo would proceed, 2) the names of all directories to be copied, 3) the deadline by which the copy is required, and 4) the name of the presentation that the copy will be used for.

k. **A member of the public has asked to copy content from a NARA web site and post it on his or her personal web site. Is this permitted?** Content on the NARA web site is in the public domain unless otherwise noted on the web page in question. Content authored by a NARA employee, unless written on personal time and owned by the employee, is NARA-owned content. It is in the public domain. The public may copy and post such content on personal web sites. However, NARA must be cited as the content source and all NARA branding must be stripped from the content. The content and design must not appear to represent NARA. Exit pages, disassociating the private web site from NARA's, must be used. See 807.6(d).

l. **We received an e-mail message telling us we won an award for our web site content. Can we add the award logo to the web site?** If the award is legitimate and can be confirmed as issued by a reputable source known for evaluating web sites for content and design, the award and its logo may be presented on the web site. However, a link between the logo or mention of the award and the organization providing the award is not permitted. See 808.13i(4) before proceeding.

m. **May we post vendors' information, such as price schedules or product lists, on a NARA web site?** NARA web sites may provide an external link to a vendor's web site if it is part of a contractual agreement or provides convenience to NARA customers. An exit page, providing a non-endorsement statement, must be used. See subpar. 807.13g for more information about external links.

National Archives and Records Administration

NARA 817
August 18, 2005

SUBJECT: Posting Digital Copies of High-Demand Archival Materials on NARA Web Sites

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a new directive establishing criteria and guidelines for the posting of archival materials on NARA web sites in response to temporary high demand from the press or public interest.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 817
August 18, 2005

SUBJECT: Posting Digital Copies of High-Demand Archival Materials on NARA Web Sites

817.1 Purpose of this directive

a. This directive establishes criteria and guidelines for the posting of archival materials on NARA web sites in response to temporary high demand from the press or due to public interest. This directive applies to individual documents that are high profile because of their content or because they provide context for a topic that is high profile.

b. This directive does not apply to bodies of material that have sustained moderate research use over time, or to images of archival materials that are used in a collage or other artwork where the text is not intended to be legible or "representative" of the material. See NARA 816, Digitizing Activities for Enhanced Access.

817.2 Authorities for this directive

a. 44 U.S.C. §§ 2108-2110, 2111note, 2112, and 2114;

b. 44 U.S. C. § 2203;

c. NARA Strategic Plan (revised 2003), Goal 3, Strategy A;

d. NARA 807, Content Rules and Requirements for NARA Public Web Sites (Internet and NARA-Hosted Extranets);

e. Preservation Guidelines for Contractors Handling Records and Historical Materials (available on the NARA intranet); and

f. NARA 816, Digitizing Activities for Enhanced Access and its supplement, Technical Guidelines for Digitizing Archival Materials for Electronic Access: Creation of Production Master Files—Raster Images

817.3 Definitions

a. **Archival materials** are records, personal papers, and artifacts in any form or media created, received, or accumulated by a person or organization in the course of the conduct of affairs, and preserved because of their continuing value.

b. **Digital surrogate** is a digital image or copy of a textual or non-textual document (e.g., scanned images of documents, digitized sound recordings).

c. **Digitization** means the creation of digital surrogates for dissemination by a variety of means, including the Internet and CD-ROM.

d. **Digitizing** refers to the act of creating a digital surrogate for dissemination by a variety of means, including the Internet and CD-ROM.

e. **NARA web sites** are the Archives.gov web site, Presidential library web sites, and other NARA web sites that include images of archival materials, such as ourdocuments.gov.

817.4 Responsibilities

a. For archival materials to be posted on the Archives.gov web site and other web sites managed by the Web Services Branch (IOW):

(1) **Research Services (R) and Legislative Archives, Presidential Libraries, and Museum Services (L)** --

(a) Identify high-demand archival materials from among their holdings, appropriate to the topic and the customer need, for posting;

(b) Provide the materials or copy of the materials to the Digitization Services Branch (IDS) for digitizing;

(c) Consult with the Office of General Counsel (NGC) as necessary to ensure that any copyright or other intellectual property right notices are made; and

(d) Ensure that a description of the archival materials and the digital surrogates are added to the Archival Research Catalog (ARC) in a timely fashion.

(2) **Web Services Branch (IOW)** --

(a) Coordinates the posting of archival materials on the Archives.gov web site;

(b) The Digitization and Description staff provides support for adding the description and copy of the archival materials to ARC;

(c) Assesses proposed location within the web site, and obtains approval by content owner;

(d) Reviews digital surrogates for accessibility and suitability for web delivery; and

(e) Posts the materials.

(3) **Digitization Services Branch (IDS)** --

(a) Creates digital surrogates based on NARA 816 and its supplement, Technical Guidelines for Digitizing Archival Materials for Electronic Access: Creation of Production Master Files—Raster Images; and

(b) Until the Electronic Records Archives (ERA) has this functionality and unless other arrangements have been approved, provides long-term storage and preservation of the master copies of the digital surrogates.

(4) **Public Affairs Director (SC)** -- determines whether a press release should be issued, and, if so, issues press release.

b. For archival materials posted on Presidential libraries web sites, **Presidential library directors --**

(1) Approve and designate the process governing the posting of archival materials on the library's web pages.

(2) Ensure that digital surrogates meet the Technical Guidelines for Digitizing Archival Materials for Electronic Access: Creation of Production Master Files—Raster Images;

(3) Consult with NGC as necessary to ensure that any copyright or other intellectual property right notices are made;

(4) Ensure that the digital surrogates meet accessibility requirements. See NARA 807, Content Rules and Requirements for NARA Public Web Sites (Internet and NARA-Hosted Extranets) for more information;

(5) Ensure long-term storage and preservation of the master copies of the digital surrogates as cited in NARA 816;

(6) Ensure that a description of the archival materials and the digital surrogate are added to the Archival Research Catalog (ARC) in a timely fashion as cited in NARA 816;

(7) Contact the Web Program Director to determine how links may be made between the library's archival materials and IOW-managed web sites; and

(8) Contact Public Affairs Director to coordinate any press releases.

817.5 How are records created by this directive maintained under the NARA records schedule?

a. R and L file records created and maintained by this directive by following the disposition instructions under category 840, NARA Web Function, in the NARA records schedule. Specifically:

(1) R uses item 840-1b.

(2) Presidential libraries use items 840-1a and 840-1b.

b. IOW uses items 840-1 and 840-2.

c. SC uses item 1002, News Releases.

d. The digital copies created by IDS are reference copies, which are nonrecord materials. See subpara. 817.4a(3)(b) for additional information.

817.6 Frequently asked questions

a. **Does NARA encourage posting digital surrogates of high-interest documents on the web sites?**

Yes. Posting digital surrogates of exceedingly high interest improves timely public access to the materials and reduces workload on the staff charged with providing reference service to those documents.

b. **How do we decide whether or not to post a digital surrogates of a document on the web sites?**

Weigh the cost associated with posting the digital surrogate against the benefit to be gained. Costs include staff time needed to digitize the document and make it compliant with accessibility requirements, and the long-term storage and preservation of the digital surrogates. Benefits include improved timely public access to high-demand documents, and reducing workload on the staff charged with providing reference access to those documents. In making this decision, focus on demand for the material, not the content of the material itself. The decision to post is made on a case-by-case basis.

c. **Is there a time factor?**

Yes. Often interest in materials peaks quickly and then subsides quickly. To best serve the press and public and relieve pressure on staff, make the decision to post digital surrogates very quickly, and post the materials as quickly after the decision as possible. Whenever possible, plan ahead to identify and prepare for this situation.

d. **Where should the digital surrogates appear on the web sites?**

Because of the high profile nature of the posting, put it on the Archives.gov or library main page. Links from other web pages may be made on a case-by-case basis by the IOW or library web staff, depending upon the nature of the document, customer demand for it and expectation of its availability and location, and current existence and location of related material on a NARA web site. For example, a digital surrogate of a recently-released very high profile 9/11 Commission staff monograph was posted on the Archives.gov web site and linked to from both the research main page and pages within the research area.

e. **Why should the document be added to ARC?**

ARC is the central repository for information about our holdings. Once interest for the document wanes and links to it from NARA web pages are removed or moved, we still want users to be able to access the digital surrogate of the document online.

f. **How long should the digital surrogate of a document be linked to from NARA web sites pages?**

This decision should be made on a case-by-case basis depending chiefly upon customer need. Also for consideration is the digital surrogate's relationship to other materials on the web site, and to content authors' available resources to conduct review and update of content accompanying the digital surrogate(s).

National Archives and Records Administration

NARA 1104
May 31, 2005

SUBJECT: Participation on Standards Bodies

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a new directive that provides policies and procedures for NARA employees serving as members of any external group or committee whose purpose is to develop standards, technical reports, or recommendations for best practices.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1104
May 31, 2005

SUBJECT: Participation on Standards Bodies

1104.1 What is the purpose of this directive?
This directive provides policies and procedures for NARA employees serving as members of any external group or committee whose purpose is to develop standards, technical reports, or recommendations for best practices. For the purposes of this directive, standards and best practices do not include professional standards of personal conduct or institutional codes of ethics. This directive supports Goal 5 of NARA's Strategic Plan.

1104.2 What is the authority for this directive?
The authority for this directive is Office of Management and Budget (OMB) Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

1104.3 When do the policies in this directive apply?

a. The policies and procedures in this directive apply when employees are serving with organizations that develop and issue formal voluntary consensus standards.

b. The policies and procedures in this directive do not apply to professional organizations such as the Society of American Archivists that do not participate in standards body work. ADMIN 201, Chapter 19, Part 2, Professional Activities, describes the policies and procedures that apply to NARA employee participation with professional organizations. The Standards Executive (see subpar. 1104.4e for a definition) can clarify whether or not this directive applies to specific organizations or activities.

1104.4 Definitions

a. Best Practices – management practices, work processes, or operating methods that have been determined to be exemplary within a specified industry or organization.

b. NARA representative – a NARA employee who acts for NARA on a standards body.

(1) Lead representative – the primary NARA representative on a standards body and the one responsible for coordinating NARA's efforts for that group.

(2) Alternative representative – a secondary NARA representative on a standards body who works closely with the lead representative and who acts in place of the lead representative when necessary.

c. Standard – something set up by an authority as a rule or principle for the measure of quantity, quality, weight, extent, or value.

d. Standards body – for the purposes of this directive, any committee, working group, or other component of a domestic or international organization whose purpose is to develop standards, technical reports, or recommendations for best practices using agreed-upon procedures that include the attributes of openness, balance of interest, due process, appeals process, and consensus. Examples include the International Organization for Standardization (ISO), AIIM (the Enterprise Content Management Association), National Information Standards Organization, and the American National Standards Institute. Also included are Federally-sponsored interagency groups such as the Federal Geographic Data Committee that develop standards for Federal agencies.

e. Standards Executive – a member of NARA's Strategy Division (SP) who coordinates NARA's participation on standards bodies, reports on NARA's standards development activities to the appropriate oversight agencies, and represents NARA on the Interagency Committee on Standards Policy (ICSP).

f. Support team – a group of NARA employees selected to provide advice and information to the NARA representatives on topics and concerns related to the standard being developed. The team often includes policy, technical, and subject experts. Team members are in close communication with the NARA representatives and need to respond quickly to information requests.

g. Technical report – a formal written account or statement detailing special and usually practical knowledge of a subject; often best practices are presented in a technical report.

h. Voluntary consensus standards – standards, technical reports, and recommendations for best practices that are planned, developed, established, or coordinated by domestic or international organizations using agreed-upon procedures that include the attributes of openness, balance of interest, due process, appeals process, and consensus. These standards include provisions requiring that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free, or reasonable royalty basis to all interested parties. Other types of standards, which are distinct from voluntary consensus standards, are "Non-consensus standards," "Industry standards," "Company standards," or "de facto standards," which are developed in the private sector but not in the full consensus process, and standards mandated by law, such as those contained in the United States Pharmacopeia and the National Formulary, as referenced in 21 U.S.C. 351.

1104.5 Responsibilities

a. NARA representatives on standards bodies, both leads and alternates,

(1) Represent NARA's interests on the standards body; including (when authorized by the Deputy Archivist) casting votes as a committee member;

(2) Actively contribute as a member of the standards body (e.g., participate in discussions, review documents, provide comments);

(3) Work closely and communicate with other NARA representatives participating on the same standards body;

(4) Maintain the NARA committee files (see par. 1104.14);

(5) Request views and assistance on items under consideration (e.g., draft standards) from the support team and other NARA technical and subject experts, as required;

(6) Provide timely reports to the Deputy Archivist and the Standards Executive and share information with interested offices;

(7) Submit, prior to signing, any agreements such as a Memoranda of Understanding or Non-disclosure Agreement to the Standards Executive for review by the Standards Executive, the Deputy Archivist, and General Counsel (NGC)**;** and

(8) Notify the Standards Executive when they can no longer serve on a standards body.

b. The Standards Executive

(1) Coordinates the selection of NARA employees as NARA representatives to standards bodies with the Deputy Archivist, office heads, staff directors, and standards bodies;

(2) Coordinates the selection of NARA employees as support team members with the Deputy Archivist, office heads, and staff directors;

(3) Provides the Deputy Archivist with recommendations for appointment of employees to standards bodies and support teams;

(4) Notifies NARA employees via their office head or staff director that they have been selected, approved, or disapproved to participate on standards bodies;

(5) Assists NARA representatives in the NARA-wide circulation of draft reports and solicitation of comments;

(6) Casts NARA votes on ballots and coordinates internal NARA review of balloted documents;

(7) Requests reports from NARA representatives for the Deputy Archivist;

(8) Provides reports on standards development activities to appropriate oversight agencies, such as OMB; and

(9) Represents NARA on the ICSP and other standards coordinating groups.

c. Office heads and staff directors

(1) Work with SP in the selection of and supervision of employees to serve as NARA representatives and as technical or subject experts on support teams;

(2) Evaluate the availability of staff to serve on standards bodies and support teams; and

(3) Adjust employees' regular duties and workloads to accommodate the employees' participation on standards bodies and recognize their standards work as part of the employees' officially assigned responsibilities.

d. NGC reviews the appointment of employees to standards bodies to determine compliance with applicable laws and regulations, including the conflict of interest laws.

e. The Deputy Archivist approves

(1) the selection of employees to be NARA representatives to standards bodies;

(2) the selection of employees to serve on support teams; and

(3) NARA ballots.

1104.6 When does NARA appoint NARA representatives to standards bodies?
The Deputy Archivist appoints one or more NARA representatives to standards bodies when consultation and participation in the development of best practices and the setting of standards is compatible with NARA's Strategic Plan, mission, authorities, priorities, and budget resources and is in the public interest. The number of individual NARA participants in a given standards activity is limited to the minimum required for effective representation of the various program, technical, or other concerns of NARA and the Federal Government.

1104.7 Must employees be appointed as a NARA representative to serve on standards bodies?
Any NARA employee serving on a standards body must do so as a duly-appointed NARA representative.

1104.8 What do I do if I am asked by an outside organization to serve on a standards body?
You must prepare a memorandum requesting to serve on the standards body. Address the memorandum to the Standards Executive, SP and route it through your proper management channels. The Standards Executive will coordinate the selection process, and the Deputy Archivist will appoint the NARA representative. Include in your request:

a. The name of the standards body and a description of its purpose;

b. The specific committee(s) on which you have been asked to serve;

c. The name and contact information of the person or organization that has asked you to serve;

d. The reason(s), if any, the person or organization offered for requesting you specifically;

e. The benefits to NARA;

f. Length of your appointment; and

g. Resources needed for you to serve (e.g., time commitment for meetings, travel funding).

1104.9 What do I do if I am asked to appoint a NARA representative to a standards body?

You must forward the request to appoint a NARA representative to the Standards Executive, SP. The Standards Executive will coordinate the selection process, and the Deputy Archivist will appoint the NARA representative. Include with the request:

a. The name of the standards body and a description of its purpose;

b. The name and contact information of the person or organization that has asked you to appoint a NARA representative;

c. Benefits to NARA;

d. Length of the appointment;

e. Level of effort required (e.g., time commitment, frequency of meetings, need for travel); and

f. Suggestions for possible NARA representatives (you may ask for volunteers).

1104.10 Do NARA representatives participate equally with other members?

a. NARA representatives serving as members of standards bodies should participate actively and on an equal basis with other members, consistent with the procedures of those bodies and guidance from the Deputy Archivist, particularly in matters such as establishing priorities, developing procedures for preparing, reviewing, and approving standards, and developing or adopting new standards. Active participation includes full involvement in discussions and technical debates, registering of opinions and, if selected, serving as chairpersons or in other official capacities. NARA representatives may vote, in accordance with the procedures of the standards body, at each stage of the standards development process unless prohibited from doing so by law or NARA.

b. In some situations, NARA's role on a standards body may be limited to observation. In these situations, the Standards Executive explains that role and its responsibilities to the NARA representatives at the time of their appointment to the standards bodies.

1104.11 Are there any limitations on participation by NARA representatives?

a. Participation by any NARA employee is subject to the laws and regulations that apply to participation by Federal employees in the activities of outside organizations. Upon request, NGC advises employees who participate on standards bodies of the limitations of such service.

b. In order to maintain the independence of standards bodies, NARA representatives must refrain from involvement in the internal management of such organizations (e.g., selection of salaried officers and employees, establishment of staff salaries, and administrative policies). NARA representatives must not dominate such bodies and must abide by rules and procedures of the standards bodies, including those regarding domination of proceedings by any individual. NARA employees must avoid the practice or the appearance of undue influence relating to their NARA representation and activities in standards bodies.

1104.12 What other issues should I be aware of if I am appointed as a NARA representative to a standards body?

Committee work in general and standards work in particular is a large responsibility. It may also become a huge time commitment. If you are a NARA representative to a standards body, be aware of the issues listed below.

a. You are representing NARA's interests on the standards body. Know why you are serving and NARA's expectations of you. Know when to seek input from the support team, Standards Executive, and Deputy Archivist.

b. You are responsible for vetting drafts for comments. Discuss with the Standards Executive when it is appropriate for you to provide comments on your own, when it is necessary to vet drafts through support team or Standards Executive, and when you need to vet through all of NARA. You need to have enough background information from NARA to participate in ad hoc votes. The Standards Executive coordinates all formal votes for NARA.

c. NARA may have multiple representatives to a standards body who serve on different technical committees or working groups. Know who the lead NARA representative is. Know who has responsibilities on different committees. Communicate with the other representatives on the standards body.

d. You are expected to actively contribute as a member of the standards body. Know the processes for the standards body on which you serve. Be informed about the issues pertaining to your standards work. You may need to conduct background research on the topic beyond that which the standards body is conducting. This research may need to include related fields or take a broader view than just the topic of the standard. Ask for assistance from the support team or

subject and technical experts when needed. Know which existing NARA policies pertain to or are affected by the standard in question. Share information with NARA about your work on the standards body.

e. You may have varying levels of participation within one standards body. You may be serving on more than one committee or subcommittee. Know what your responsibilities are to each committee or subcommittee. Are you observing, participating, lead, or alternate? Be aware that you may assume several roles within one committee and may need to differentiate those roles when communicating (e.g., you're the Chair, the NARA representative, and the U.S. representative).

f. Once appointed, you may be asked to assume additional duties or change assignments in the standards body. Coordinate any changes with the Standards Executive.

g. Be aware of perceptions. You are the voice of NARA. You may also be perceived as representing the U.S. or the Federal Government. Take seriously your role as a NARA representative. Be aware of different stakeholder groups and which one(s) you represent or are perceived to represent. Pay particular attention to your actions and communications. Also be cognizant of your own perceptions of other people and groups.

h. Encourage the use of plain language in any product that will be disseminated.

i. Your work on the standards body may create requests for you to give presentations to external groups. You must obtain NARA approval to give them.

1104.13 What forms of support may NARA provide to NARA representatives?

a. NARA support for NARA representatives may include the following:

(1) Travel costs;

(a) All travel must be conducted in accordance with NARA's travel policies (see NARA Directives, Series 600 – Travel).

(b) SP, on behalf of the Archivist, coordinates and funds all international travel.

(c) Offices and Staffs fund all domestic travel.

(2) Technical support (e.g., cooperative testing for standards evaluation and participation of NARA personnel in the activities of standards bodies); and

(3) Use of facilities.

b. Supervisors should make every effort, within resource limits and workload considerations, to provide official time and travel funds, subject to the Office of Personnel

Management guidelines, to employees serving as NARA representatives. If supervisors do not have the resources necessary to support the participation of their employee(s) on a standards body, they must notify the Standards Executive.

c. If additional support is needed for a specific event (e.g., hosting a meeting), the representative must submit a request to the Standards Executive. Each request will be evaluated on a case-by-case basis.

1104.14 How are records created by this directive maintained under NARA's records schedule?

Maintain records created by this directive in accordance with Files 203, Appendix 1, Sections 115 - 117, Committees.

National Archives and Records Administration

NARA 1310
May 22, 2008

SUBJECT: Review of Agency Records Storage Facilities

TO: Executives, Staff Directors, NHPRC, and OIG

Purpose of this transmittal memo. This transmits a revised policy directive containing the internal NARA procedures for ensuring the compliance of Federal agency records storage facilities with NARA regulations in 36 CFR part 1234.

What changes are made?

a. The directive has been updated to reflect changes in the regulations that were made in 2005. These are primarily date changes.

b. The requirement in par. 1310.5 to publish the Central Registry of Records Storage Facilities on the Records Management web page and references in other paragraphs to the web page, have been removed. NARA has determined that publication of the registry on the web gives agencies the misimpression that non-NARA facilities listed in the registry were automatically "approved" for use by other Federal agencies. Each agency must individually self-certify and report compliance to NARA. Certain agency records centers (e.g., Energy) are unavailable to other agencies and certain agencies do not want their records centers listed for security reasons. Because the list included one commercial facility, it left the misimpression that NARA certifies commercial records storage facilities.

c. Appendix A will be revised at a later date.

Canceled directives. This directive cancels the policy portion of NARA 1310, dated September 6, 2000. However, Appendix A, dated September 6, 2000, remains in effect.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

NARA 1310
May 22, 2008

SUBJECT: Review of Agency Records Storage Facilities

1310.1. What is the purpose of this directive?
This directive establishes internal NARA procedures for ensuring the compliance of Federal agency records storage facilities with NARA regulations in 36 CFR 1234.

1310.2 What is the authority for this directive?

a. NARA is authorized to:

(1) Establish, maintain, and operate records centers for Federal agencies under 44 U.S.C. 2907;

(2) Approve agency records centers under 44 U.S.C. 3103; and

(3) Promulgate standards, procedures, and guidelines to Federal agencies with respect to the storage of their records in commercial records storage facilities (see 44 U.S.C. 2104(a), 2904 and 3102).

b. NARA regulations in 36 CFR 1234, specify the facility standards and approval processes that apply to all records storage facilities Federal agencies use to store, service, and dispose of their records.

1310.3 Definitions.
As used in this directive:

a. ***Agency records center*** means a records center not operated by NARA that is established and operated by a Federal agency for its own records and/or the records of other Federal agencies, or Federally owned and contractor-operated.

b. ***Commercial records storage facility*** means a private sector commercial facility that offers records storage, retrieval, and disposition services.

c. ***Existing facility*** means a records storage facility used to store records on September 27, 2005, and that has stored records continuously since that date.

d. ***NARA records center*** means a records center operated by NARA, including the Washington National Records Center and the National Personnel Records Center.

e. ***New facility*** means a records storage facility established or converted for use as a

records center or commercial records storage facility on or after September 28, 2005.

f. ***Records storage facility*** means a NARA records center, an agency records center, or a commercial records storage facility.

g. 36 CFR part 1234, including any appendixes to the part.

1310.4 Responsibilities

a. The Storage Coordination and Logistics Branch (BFS) is responsible for:

(1) Facility inspections and documentation reviews for records storage facilities;

(2) Approval or denial of waivers of NARA facility standards and alternative fire detection and suppression systems, consulting with appropriate industry standards body or other qualified expert(s) as needed to determine the adequacy of proposed alternatives to published NARA standards;

(3) Maintaining the files described in pars. 1310.5a through 1310.5d as the central registry of records storage facilities used to store Federal records.

(4) Approving agency plans to bring noncompliant agency records centers into compliance;

(5) Confirming that an agency has removed its records from a noncompliant records storage facility within the time limits specified in 36 CFR 1222.50(c)(3); and

(6) Notifying an agency when NARA learns that the agency is using a records storage facility without obtaining NARA approval (see par. 1310.12).

b. The National Records Management Program (ACN) is responsible for notifying BFS:

(1) When an agency submits a records schedule for unscheduled records that will be stored in an agency records center or commercial records storage facility;

(2) If it learns that an agency is storing records in a facility not listed as approved on the BFS central registry of records storage facilities; and

(3) If it observes obvious non-compliances with 36 CFR 1234 in a records storage facility when staff visit the facility to review records as part of processing a records disposition request or while conducting an agency evaluation or technical assistance project.

c. The Chief Records Officer (AC) is responsible for reviewing agency documentation for permanent records stored in off-site facilities compiled in accordance with 36

CFR 1228.154(c) and providing copies to other units with an interest in the information.

d. The Records Center Program Director (AF) is responsible for notifying:

(1) BFS and ACN whenever an agency announces its intention to withdraw its holdings from a NARA records center or no longer regularly transfers additional records to a NARA records center; and

(2) BFS if it learns that an agency is storing records in a facility not listed as approved on the BFS central registry of records storage facilities.

1310.5 What is the central registry of records storage facilities and how is it updated?

The files described in pars. 1310.5a through 1310.5d comprise the central registry of records storage facilities reviewed by BFS. BFS modifies the registry as facilities are approved or disapproved. BFS provides a current report of approved records storage facilities (see par. 1310.5a) to ACN and AF each quarter, and notifies those offices of updates to the database whenever additional facilities are approved or removed from the approved facility database.

a. BFS maintains a database and generates a quarterly report that includes the following elements for each approved records storage facility:

(1) Name and address of the facility;

(2) Date approved by BFS, if a NARA records center or agency records center, or date BFS completed its review of an agency's certification of compliance for a commercial facility;

(3) Agency(ies) that have obtained NARA approval (agency records center) or submitted certifications of compliance (commercial storage facility) for this facility and the name and address of the agency contact (BFS does not maintain this information on agencies that use a NARA records center);

(4) Waivers granted, if any; and

(5) Compliance requirements that will take effect October 1, 2009, that the facility does not currently meet, if any.

b. BFS maintains a case file for each approved records storage facility that contains:

(1) The agency request for approval and any documentation submitted with that request;

(2) A copy of the completed BFS checklist (see Appendix A);

(3) The official file copy of any correspondence relating to review of a waiver

or alternative fire detection and suppression system; and

(4) The official file copy of BFS's approval letter to the agency.

c. BFS maintains an electronic list of records storage facilities for which NARA approval has been withdrawn or that did not receive NARA approval because of documented noncompliance with a facility requirement in 36 CFR part 1234. This information is not maintained as part of the database listing described in subpar. a. BFS maintains the supporting documentation for each disapproved facility in a separate case file.

d. BFS maintains a file on each fire detection and suppression system that BFS has certified as compliant with 36 CFR 1234.14(s). The file contains either

- the report of the results of independent live fire testing, or
- the report of the results of computer modeling and certification required by 36 CFR 1234(a)(3).

1310.6 What types of reviews does BFS perform?

BFS performs the following types of reviews:

a. Reviews of 36 CFR 1234 compliance – BFS reviews documentation and/or inspects records storage facilities to assess their compliance with the requirements in 36 CFR 1234.10 through 1234.20. Paragraph 1310.8 specifies how BFS conducts the review for agency and NARA records centers. Paragraph 1310.10 specifies how BFS conducts this review for commercial storage facilities.

b. Reviews of waiver requests – BFS reviews documentation submitted with requests for waivers from specific requirements in 36 CFR 1234 to determine whether to approve an exception to a standard in 36 CFR 1234 for:

(1) Systems, methods, or devices that are demonstrated to have equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety to those prescribed by this part("equivalent or superior alternative");

(2) Existing agency records centers that met the previous NARA standards in effect on January 2, 2000, but that do not meet a new standard required to be in place on September 28, 2005;

(3) The application of roof requirements in 36 CFR 1234.10 and 1234.12 to underground storage facilities; or

(4) Conflicts between NARA standards and either local/regional building codes or mandatory 30 CFR chapter I life-safety/ventilation requirements for underground storage facilities.

c. Reviews of plans to bring noncompliant agency records centers into compliance --

Under 36 CFR 1234.30(d), BFS reviews plans submitted by agencies to bring unapproved existing agency records centers into compliance with current 36 CFR 1234 requirements.

1310.7 What are the time limits for BFS action?

a. For reviews of 36 CFR 1234 compliance and reviews of plans to bring noncompliant agency records centers into compliance, BFS must respond to the agency with an approval or disapproval within 45 calendar days after receiving the request. This time limit may be extended if:

(1) Complete supporting documentation is not provided with the request (the 45-day time limit starts when the complete documentation is received);

(2) BFS must consult an industry standards body or qualified expert to determine whether the supporting documentation demonstrates compliance with 36 CFR 1234.12(s) (the time limit is extended to 75 days);

(3) BFS is not able to schedule an inspection of the facility within the first 30 days (BFS must complete the review within 15 days after the inspection is held); or

(4) The agency is also requesting a waiver from a 36 CFR 1234 requirement (see par. 1310.7b for the number of days that are added to the 45-day time limit).

b. For reviews of waiver requests, BFS must respond to the agency within the following time limits:

Type of waiver request	**Time limits (calendar days)**
Equivalent or superior alternative to NARA requirement	30 days (Initial notification if NARA must consult an industry standards body or qualified expert.) 60 days (Final determination if consultation is needed.)
Existing approved agency records center does not meet new standard	30 days (BFS may grant a short-term temporary waiver of up to 180 days if the agency's plan must be revised before NARA approval.)
Roof requirements for underground storage facilities	10 days (unless the agency has also requested another waiver)
Code conflicts	30 days

1310.8 How does BFS inspect NARA records centers and agency records centers for compliance with 36 CFR 1234?

a. BFS conducts an initial inspection of existing agency records centers as follows. An inspection team from BFS (General Engineer and another member of BFS with experience in fire safety) or a professional engineering firm on contract to BFS physically inspects the facility using the facility checklist in Appendix A. The facility director or designated representative signs the facility checklist and may provide a statement of disagreement or clarifications to the

checklist findings. The inspection team or contractor informally discusses its findings with the agency before the end of the inspection visit. The completed checklist and any supplementary notes on corrective action that must be taken to bring the facility into compliance with 36 CFR 1234 serve as the inspection report. The Director, BFS reviews the inspection report and determines whether to approve the facility or to require corrective action before granting approval. BFS may issue a conditional approval that allows use of the facility while corrective actions are being made if there is no immediate danger to the records to be stored in the facility.

b. BFS reviews the 100% construction drawings and specifications and proposed shelving plan for new NARA records centers and agency records centers. If this review confirms design compliance, BFS grants conditional approval. BFS inspects new NARA records centers upon completion of construction or renovation. Upon completion of construction of an agency records center, the agency must either submit an Architect and Engineer (A&E) certification that the facility was in fact constructed in accordance with the approved design documents or request a BFS inspection. If the review of the A&E certifications demonstrates full compliance, BFS issues final approval. If the agency prefers an onsite inspection, the inspection must be in accordance with subpar. b.

c. BFS conducts a full onsite physical inspection of each approved agency records center and NARA records center every 10 years or within 6 months after BFS is notified that a material change in the center has occurred. For approved facilities that must be modified to comply with roof, piping, or environmental control requirements that become effective October 1, 2009, BFS conducts an onsite physical inspection of the facility no later than March 31, 2010, to verify that the facility is in compliance with those phased-in requirements.

1310.9 What documentation is required to assure compliance of commercial facilities with 36 CFR 1234?

The agency must submit:

a. A copy of the contract incorporating (in mandatory terms) 36 CFR 1234 or a certification of compliance signed by the agency records officer. The GSA multiple award schedule for records centers (MAS) contract currently does not meet this requirement.

b. A description of the fire suppression system. If the facility is not listed as approved in the BFS central registry of records storage facilities, BFS also requires one of the following forms of documentation:

(1) Appendix B systems: The agency must submit a statement signed by a responsible official (i.e., Records Officer or agency Safety Officer) that the system complies fully with a system described in Appendix B of 36 CFR 1234. BFS inspects the system during the first three years after NARA approval.

(2) Tested systems: The agency must submit a report from the testing lab, which may be accompanied by an additional report from a Fire Protection Engineer (FPE). BFS reviews the report(s). If the test clearly shows less than 300 cubic feet of records destroyed, BFS approves the system. If the report does not clearly distinguish between "involved" and

"destroyed," BFS may seek additional clarification. If tests show clear failure, BFS does not approve the facility.

(3) Modeling/certification by FPE: The agency submits a full report of modeling, FPE's report, and certification. BFS verifies the FPE's status by means of a computer check of the FPE's registration. BFS reviews the modeling for completeness, compliance with ANSI standards, etc. BFS consults with the FPE that conducted the modeling if there are any questions about the certification. If BFS still has questions, BFS consults with the appropriate industry standards body or other qualified expert before approving or disapproving the system.

(4) Copy of previously approved system: The agency submits a certification from a responsible agency official (agency Records Officer or Safety Officer) that the system is an exact copy of a previously approved system.

c. A description of the security system.

d. A description of the shelving arrangement (height, whether pallets are used, etc.).

e. A description of the environmental controls and the type(s) of records to be stored. For new facilities, this information must be provided for all records. For existing facilities, until October 1, 2009, the agency must provide the information only if nontextual permanent records will be stored in the facility. After September 30, 2009, agencies must provide the information for all facilities and records.

1310.10 How does BFS review agency documentation for commercial records storage facilities?

BFS registers the request on the date received in BFS. Within 15 calendar days, BFS reviews the name and address of the facility against the BFS central registry of records storage facilities for approved and noncompliant facilities, and verifies that the documentation contains the information specified in par. 1310.9.

a. If the facility is on the approved list, BFS notifies the agency in writing that the facility is compliant. If the facility appears on the list of noncompliant facilities, BFS notifies the agency that we have previously found the facility to be noncompliant in specific areas. BFS asks the agency to confirm in writing to BFS within 30 days that nonconformances have been corrected. BFS sends the notification within 2 workdays after the review is complete.

b. If the facility is not on either list, BFS reviews the documentation submitted with the request to ensure that the documentation specifies compliance with 36 CFR 1234. Par. 1310.9 specifies the content of the required documentation. BFS also reviews any other readily available information about the facility (e.g., whether it is an underground facility). BFS completes its review and notifies the agency in writing within 45 calendar days of the approval of the facility or of the areas in which the facility appears to be not in compliance with 36 CFR 1234. If the documentation is incomplete (e.g., there is no description of the fire suppression system, security system, or shelving arrangement), BFS asks the agency to correct the deficiencies so that NARA can complete its review.

1310.11 How does BFS process requests for waivers made under 36 CFR 1234.22?

a. Code conflicts.

(1) Agency documentation must contain:

(a) A concise explanation of the conflict;

(b) Citation to the code in conflict (if not available from normal sources or on the Internet, NARA may request a copy of the code document); and

(c) Either a demonstration that the code in conflict is more stringent or a demonstration that the conflicting code is mandatory and cannot be reconciled with the NARA requirement (e.g., letter from the authority having jurisdiction [building inspector, fire marshal, etc.]).

(2) BFS review:

(a) If the claim is that the conflicting code is mandatory, BFS reviews to ensure that the documentation is complete and supports the claim. If the documentation is incomplete, BFS sends a letter to the agency within 5 workdays requesting the missing information. If BFS has questions about the claim, BFS reviews the code in conflict and may consult with a professional engineer licensed in that State for review of the provisions, especially with regard to lack of flexibility in the local code.

(b) If the claim is that the conflicting code is more stringent, BFS reviews the claim in accordance with par. 1310.11b(2).

b. Equal or superior protection.

(1) Agency documentation must contain:

(a) A concise explanation of the alternative, including why the requester feels the alternative provides equal or superior protection; and

(b) Supporting documentation in one of the following forms: a testing report, a Fire Protection Engineer's report, or the agency Safety Officer's written determination.

(2) BFS reviews the testing results or other documentation for compliance with ANSI or other appropriate standards. If the documentation is incomplete, BFS sends a letter to the agency within 5 workdays requesting the missing information. If BFS has questions about the claim, BFS requests outside expert review.

c. Grandfather claims.

(1) Agency documentation must contain:

(a) Concise statement of how the facility met the previous requirements, but does not meet the new regulations (most likely to involve environmental controls or pest management), and

(b) Action plan with milestones, funding requirements, and a description of how the corrections will be funded. (The action plan must provide for correction to be completed within three years.)

(2) BFS reviews the documentation. If all required elements are present and the action plan appears feasible, BFS approves the waiver. If the documentation is incomplete or the description of the corrective action is not sufficiently detailed, BFS sends a letter to the agency within 5 workdays requesting the missing information. If the corrective action is not scheduled for completion within three years, BFS denies the waiver request.

d. Waivers of roof-related requirements for underground facilities.

(1) The agency documentation must include a description of the facility (drift or shaft) and its location.

(2) BFS reviews the documentation. If complete, BFS approves the waiver. If the documentation is incomplete, BFS sends a letter to the agency within 5 workdays requesting the missing information.

1310.12 How does BFS handle notifications that an agency is storing records in an unapproved facility?

a. When ACN or AF notify BFS that an agency intends to store, or is storing, records in a facility that is not on the list of approved records storage facilities, BFS sends a letter to the agency records officer reminding the agency of the approval requirements in 36 CFR 1234.30. The letter asks the records officer to submit the approval request within 45 calendar days or to contact BFS before that date to establish a later submission date.

b. If the agency records officer does not respond to the BFS letter within 55 calendar days, BFS prepares a letter to the head of the agency for the Archivist's signature. The letter informs the agency head that the agency has not complied with 36 CFR 1234.30 and that the agency must either take steps immediately to remove its records from the facility or submit the approval request. The agency head has 30 calendar days to respond. If the agency head fails to respond to the Archivist's request for information within that time frame, BFS will advise the NARA Inspector General (OIG) and request that the OIG notify the Inspector General or equivalent entity of the non-responsive agency.

c. BFS copies ACN and AF on all correspondence.

1310.13 How does BFS monitor agency removal of records from noncompliant

facilities?

a. Under 36 CFR 1222.50(c)(3), agencies are responsible for initiating action to remove records from space that does not meet the standards if deficiencies are not corrected within 6 months after initial discovery of the deficiencies by NARA or the agency. Agencies must complete removal of the records within 18 months after initial discovery of the deficiencies.

b. If BFS discovers, on its own or through notification by an agency, deficiencies that render a records storage facility noncompliant, BFS promptly notifies the records officer in each agency that stores records in that facility, copying ACN and AF on the letter. The BFS notification letter informs the agency(ies) that the agency must provide, within 6 months of the date of the letter, either documentation to BFS that the deficiency has been corrected or the agency's plan to remove the records from the facility. A plan to remove the records must be started no later than 6 months of the date of the letter and scheduled for completion within 18 months of the date of the BFS letter. The agency may send the removal plan, initial removal notification, and notification that all records have been removed via letter or email to BFS.

c. BFS establishes a tickler file for each noncompliant facility. BFS reminds the agency records officer(s) one month in advance of the due dates to provide documentation, a removal plan, or removal notifications. If BFS does not receive the required material within 10 workdays after the due date, BFS follows up with the records officer by telephone or email. If BFS still does not receive the required material or a request for a reasonable extension within 20 workdays of the original due date, BFS prepares a letter to the agency head for the Archivist's signature. The letter informs the agency head that the agency's records are stored in a noncompliant facility and what steps the agency must complete. BFS will also advise the OIG and request that the OIG notify the Inspector General or equivalent entity of the noncompliant agency.

d. BFS copies ACN and AF on all correspondence. BFS informs ACN and AF of actions taken.

Appendix A

Facility Standards for Records Storage Facilities Inspection Checklist

Complete all sections of this checklist for the commercial records storage facility. Also complete either Supplemental Checklist for Appendix B Fire-Safety Systems or provide the information required by 36 CFR 1234.10.

Facility Standards for Records Storage Facilities Inspection Checklist (Effective date of checklist September 2005)		
Agency:		
Facility:	Common Name:	
	Street Address	
	City, State & Zip	
	Facility description (size and capacity):	
Facility Director or Representative:	☐ Comments explaining or disagreeing with inspection findings are attached.	
Inspector or Reviewer:	_____ _____ Date _____ _____ Date INSPECTION/REVIEW DATE:	

List of Attachments		
Description	Yes	N/A
Supplemental Checklist for Appendix B Fire-Safety Systems		
Certification of fire-safety detection and suppression system (36 CFR 1234.32)		
Exceptions caused by Code Conflicts (36 CFR 1234.20)		
Waiver request(s) (36 CFR 1234.22)		
Other: (Describe)		

Section 1 - Compliance with 36 CFR 1234.10 Facility Requirements				
§1234.10 paragraph:	Requirement	OK	No	Other
(a)	The facility must be constructed with non-combustible materials and building elements, including walls, columns, and floors.			
(a) exception 1	If the roof is constructed of combustible material it is protected by a properly installed and maintained wet-pipe automatic sprinkler system.			
(a) exception 2	Existing records storage facility with combustible building elements has an approved waiver from BX that allows continued use until October 1, 2009 provided documentation has been submitted that indicates a fire-suppression system designed to mitigate the risk is present.			
(b)	A facility with two or more stories must be designed or reviewed by a licensed fire protection engineer and civil/structural engineer to avoid catastrophic failure of the structure due to an uncontrolled fire on one of the intermediate levels.			
(c)	The building must be sited a minimum of five feet above and 100 feet from any 100 year flood plain areas, or be protected by an appropriate flood wall (see FEMA flood maps)			
(d)	The facility must be designed in accordance with national, regional, state or local building codes (whichever is most stringent) to provide protection from building collapse or failure of essential equipment from earthquake hazards, tornadoes, hurricanes, and other natural disasters.			
(e)	Roads, fire lanes, and parking areas must permit unrestricted access for emergency vehicles.			
(f)	A floor load limit must be established for the records storage area by a licensed structural engineer. … The allowable load limit must be posted in a conspicuous place and must not be exceeded.			
(g)	The facility must ensure that the roof membrane does not permit water to penetrate the roof. (New buildings: effective 9/28/2005; existing buildings: effective 10/1/2009)			
(h)	Piping (with the exception of sprinkler piping and limited storm water roof drainage piping – see 36 CFR 1234.10(h) of the rule for further information) must not be run through the records storage area unless supplemental measures … are used to prevent water leaks … . (New buildings: effective 9/28/2005; existing buildings: effective 10/1/2009)			
(i)(1)	All racking systems, steel shelving, or other open-shelf records storage equipment must be designed and installed to provide seismic bracing that meets the requirements of the applicable state, regional, and local building code (whichever is most stringent).			
(i)(2)	Racking systems, steel shelving, or other open-shelf records storage equipment must be braced to prevent collapse under full load. Each racking system or shelving unit must be industrial style shelving rated at least 50 lbs per cubic foot supported by the shelf.			
(i)(3)	Compact shelving, if used, must be designed to permit proper air circulation and fire protection …			
(j)	The records storage area must be equipped with an anti-intrusion alarm system … meeting the requirements of UL 1076, Proprietary Burglar Alarm Units and Systems (level AA) …. The alarm system must be monitored in accordance with UL 611, Central Station Burglar Alarm Systems.			

Section 1 - Compliance with 36 CFR 1234.10 Facility Requirements				
§1234.10 paragraph:	Requirement	OK	No	Other
(k)	The facility must comply with the requirements for a Level III facility. (**36 CFR 1234 Appendix A** -- see Section 4 of this Checklist)			
(l)	Records contaminated by hazardous materials … must be stored in separate areas having separate air handling systems from other records.			
(m)	The facility must have an Integrated Pest Management program.			
(n)	The following additional requirements apply only to new facilities:			
(n.1)	(1) No mechanical equipment containing motors in excess of 1 HP within records storage areas (excluding material handling and conveyance equipment that have operating thermal breakers on the motor).			
(n.2)	(2) No high-voltage electrical distribution equipment (i.e., 13.2kv or higher) in records storage areas.			
(n.3)	(3) A redundant source of primary electrical service … should be provided … . Manual switching between sources of service is acceptable. (See text in rule; applies to HVAC, fire and security alarms.)			
(n.4)	(4) For new facilities that store permanent records:			
requirement a.	a. A facility storing permanent records must be kept under positive pressure.			
requirement b.	b. No intake louvers in loading dock areas, parking or other areas subject to vehicle traffic.			
requirement c.	c. Separate air supply and exhaust system for loading docks.			

Section 2 - Compliance with 36 CFR 1234.12 Fire Safety Requirements				
§1234.12 paragraph:	Requirement	OK	No	Other
(a)	The fire detection and protection system must be designed or reviewed by a licensed fire protection engineer. Review requires submission of a report under the seal of a licensed fire protection engineer; see rule text for minimum requirements.			
(b)(1)	All walls separating records storage areas from each other and from storage areas within the building must be at least 3-hour fire barrier walls.			
(b)(2)	The quantity of Federal records stored in a single records storage area must not exceed 250,000 cubic feet.			
(c)(1)	For existing records storage facilities, at least 1-hour rated fire barrier walls must be provided between the records storage area(s) and other auxiliary spaces.			
(c)(2)(*a*)	For new records storage facility, 2-hour-rated fire barrier walls must be provided between the records storage area(s) and other auxiliary spaces.			

Section 2 - Compliance with 36 CFR 1234.12 Fire Safety Requirements				
§1234.12 paragraph:	Requirement	OK	No	Other
(c)(2)(*b*)	For new facilities, at least one exterior wall of each stack area must be designed with a maximum fire resistive rating of one-hour, or, if rated more than one-hour, there must be at least one knock-out panel in one exterior wall of each stack.			
(d)	Penetrations in the walls must not reduce the specified fire resistance ratings.			
(e)	The fire resistive rating of the roof must be a minimum of ½ hour.			
(e) alternate	Unrated roof is protected with an automatic sprinkler system in accordance with NFPA 13.			
(f)	Openings in fire barrier walls must be protected by self-closing or automatic Class A fire doors, or equivalent doors that maintain the same rating as the wall.			
(g)	Roof support structures that cross or penetrate fire barrier walls must be cut and independently supported on each side of the fire barrier wall.			
(h)	If fire barrier walls are erected with expansion joints, the joints must be protected to their full height.			
(i)	Building columns in records storage areas must be 1-hour fire resistant.			
(i) alternate	Unrated columns are protected in accordance with NFPA 13.			
(j)(1)	Automatic roof vents for routine ventilation purposes must not be designed into new records storage facilities.			
(j)(2)	Automatic roof vents, designed solely to vent in the case of a fire, with a temperature rating of at least twice that of the sprinkler heads are acceptable.			
(k)	Where lightweight steel roof or floor supporting members are present, they must be protected either by applying a 10-minute fire resistive coating to the top chords of the joists, or by retrofitting the sprinkler system with large drop sprinkler heads. (see rule text)			
(l)	Open flame (oil or gas) unit heaters or equipment, if used, must be installed or used in any records storage area in accordance with NFPA 54 and the Uniform Mechanical Code.			
(m)	For existing records storage facilities, boiler rooms or rooms containing equipment operating with a fuel supply … must be separated from records storage areas by a 2-hour rated fire barrier wall with no openings directly from those rooms to the records storage area(s). Such areas must be vented directly outside to a location where fumes will not be drawn back into the facility.			
(n)	For new records storage facilities, boiler rooms or rooms containing equipment operating with a fuel supply … must be separated from records storage areas by a 4-hour rated fire barrier wall with no openings directly from those rooms to the records storage area(s). Such areas must be vented directly outside to a location where fumes will not be drawn back into the facility.			
(o)	For new records storage facilities, fuel supply lines must not be installed in areas containing records, and must be separated from such areas with 4-hour-rated construction.			
(p)	Equipment rows running perpendicular to the wall must comply with NFPA 101 Life Safety Code, with respect to egress requirements.			
(q)(1)	No oil-type transformers, except thermally protected devices included in light ballasts, may be installed in records storage areas.			

Section 2 - Compliance with 36 CFR 1234.12 Fire Safety Requirements				
§1234.12 paragraph:	Requirement	OK	No	Other
(q)(2)	All electrical wiring must be in metal conduit, except that armored cable may be used where flexible wiring connections to light fixtures are required			
(q)(3)	Battery charging areas for electric forklifts must be separated from records storage areas with at least a 2-hour rated fire barrier wall.			
(r)	Hazardous materials … must not be stored in records storage areas.			
(s)	All records storage and adjoining areas must be protected by a professionally designed fire-safety detection and suppression system that is designed to limit the maximum anticipated loss from any single fire event to a maximum of 300 cubic feet of records destroyed. • For systems in accordance with **36 CFR 1234 Appendix B**, attach Supplemental Checklist for Appendix B Fire-Safety Systems. For other designs, see § 1234.32 for documentation requirements.			

Section 3 - Compliance with 36 CFR 1234.14, Environmental Control Requirements				
§1234.14 Paragraph:	Requirement	OK	No	Other
(a)	Paper-based temporary records must be stored under environmental conditions that prevent the active growth of mold. (See rule text)			
(b)	Nontextual temporary records, including microforms and audiovisual and electronic records, must be stored in records storage space that will ensure their preservation for their full retention period. Effective 09/28/2005 for new records storage facility and 10/1/2009 for existing facilities. (See rule text)			
(c)	Paper-based permanent, unscheduled, and sample/select records must be stored in records storage space that provides 24 hour/365 days per year air conditioning equivalent to that required for office space. (See rule text) Effective date: New facilities 09/28/2005; existing facilities 10/1/2009			
(d)	Nontextual permanent, unscheduled and/or sample/select records: see parts 1238, 1237,, and/or 1236 of 36 CFR Chapter XII.			

Section 4 - Minimum Security Requirements (Appendix A)

Compliance with Federal Facility Security Standards, Level III

For explanation of Requirements, see File 6 of this Toolkit or http://www.archives.gov/about/regulations/part-1228/appendix-a.html

Citation	Requirement	OK	No	Partial
S1	Control of facility parking			
S2	Receiving/shipping procedures			
S3	Intrusion detection system with central monitoring			
S4	Meets *Life Safety Standards*			
S5	Adequate exits from records storage areas			
S6	High security locks on entrances/exits			
S7	Visitor control/screening system			
S8	Prevent unauthorized access to utility areas			

Section 4 - Minimum Security Requirements (Appendix A)

Compliance with Federal Facility Security Standards, Level III

For explanation of Requirements, see File 6 of this Toolkit or http://www.archives.gov/about/regulations/part-1228/appendix-a.html

Citation	Requirement	OK	No	Partial
S9	Provide emergency power to critical systems			
S10	Conduct background security checks and/or establish security control procedures for service contract personnel			

Notes – use this space to add information about "Other" and "Partial" answers in Sections 1 through 4 of the Checklist

Reference (§ and ¶)	Comments

Supplemental Checklist for Appendix B Fire-Safety Systems Compliance with 36 CFR Part 1234 Appendix B (Complete this checklist ONLY if the facility claims to be using the system described in Appendix B)				
Paragraph	Requirement	OK	No	Partial
2a.	The records storage height must not exceed the nominal 15 feet (+/- 3 inches) records storage height.			
2b.	All records storage and adjoining areas must be protected by automatic wet pipe sprinklers.			
2c.	1. The sprinkler system must be rated at no higher than 285 degrees Fahrenheit utilizing quick response (QR) fire sprinkler heads.			
	2. The sprinkler system must be designed by a licensed fire protection engineer to provide the specified density for the most remote 1,500 square feet of floor area at the most remote sprinkler head in accordance with NFPA 13 (1996), Standard for the Installation of Sprinkler Systems.			
	3. Installation of the sprinkler system must be in accordance with NFPA 13 (1996), Standard for the Installation of Sprinkler Systems.			
	4. Contractor's Material and Test Certificates per NFPA 13 chapter 8.			
	5. Hydraulic Calculations.			
2d.	1. Maximum spacing of the sprinkler heads must be on a 10-foot grid.			
	2. The positioning of the heads must provide complete, unobstructed coverage, with a clearance of not less than 18 inches, but not more than 60 inches, from the top of the highest stored materials.			
2e.	The sprinkler system must be equipped with a water-flow alarm connected to a continuously staffed fire department or central station, with responsibility for immediate response.			
2f.	1. A manual fire alarm system must be provided with central station services or other automatic means of notifying the municipal fire department.			
	2. A manual alarm pull station must be located adjacent to each exit.			
2g.	All water cutoff valves in the sprinkler system must be equipped with automatic closure alarm connected to a continuously staffed station, with responsibility for immediate response.			
2h.	A dependable water supply free of interruption must be provided. This normally requires a backup supply system having sufficient pressure and capacity to meet both fire hose and sprinkler requirements for 2 hours.			

Supplemental Checklist for Appendix B Fire-Safety Systems Compliance with 36 CFR Part 1234 Appendix B (Complete this checklist ONLY if the facility claims to be using the system described in Appendix B)				
Paragraph	Requirement	OK	No	Partial
2i.	Interior stand-pipe stations equipped with 1 ½ inch diameter hose may be provided in the records storage areas if required by the local fire department, enabling any point in the records storage area to be reached by a 50-foot hose stream from a 100-foot hose lay. If hose is provided, the cabinets must be marked "For Fire Department Use Only."			
2j.	Where fire hose cabinets are not required, stand-pipes must be provided at each floor landing in the building core or stair shaft. Hose outlets must have easily removable adapter and cap. Threads and valves must be compatible with the local fire department's equipment. Spacing must be so that any point in the records storage area can be reached with a 50-foot hose stream from a 100-foot hose lay.			
2k.	In addition to the designated sprinkler flow demand, 500 gpm must be provided for hose stream demand. The hose stream demand must be calculated into the system at the base of the main sprinkler riser.			
2l.	1. Fire hydrants must be located within 250 feet of each exterior entrance or other access to the records center that could be used by fire-fighters.			
	2. All hydrants must be at least 50 feet away from the building walls and adjacent to a roadway usable by fire apparatus. Fire hydrants must have at least two 2-½ inch hose outlets and a pumper connection. All threads must be compatible with local standards.			
2m.	Portable water-type fire extinguishers (2½ gallon stored-pressure type) must be provided at each fire alarm striking station (see also NFPA 10).			
2n.	1. Where provided, the walking surface of the catwalks must be of expanded metal at least 0.09-inch thickness with a 2-inch mesh length. The surface opening ratio must be equal or greater than 0.75.			
	2. The sprinkler water demand for protection over bays with catwalks where records are not oriented perpendicular to the aisles must be calculated to give 0.3 gpm per square foot for the most remote 2,000 square feet.			

Notes for Supplemental Checklist	
Reference	Comments

National Archives and Records Administration

NARA 1403
December 13, 2006

SUBJECT: Maintenance, Disposition, and Access to Records of Defunct Executive Agencies Stored in NARA Federal Records Centers

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits the new policy directive, NARA 1403, Maintenance, Disposition, and Access to Records of Defunct Executive Agencies Stored in NARA Federal Records Centers

Why are we issuing this directive? This directive provides detailed procedures to staff regarding the maintenance, disposition, and access to records of defunct Executive agencies stored in NARA Federal Records Centers. This directive **does not** pertain to papers and records of Presidential commissions and committees that are held by the Presidential libraries and papers and records of legislative commissions and committees that are held by the Center for Legislative Archives.

Significant changes. This directive includes the following updated procedures:

- This directive will cancel 1464.14 in NARA 1464, Destruction of Federal Records in the Custody of NARA Records Centers, which contains information on obtaining agency concurrence for the disposal of records of defunct agencies.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1403
December 13, 2006

SUBJECT: Maintenance, Disposition, and Access to Records of Defunct Executive Agencies Stored in NARA Federal Records Centers

1403.1 What is the purpose of this directive?
This directive establishes the National Archives and Records Administration's (NARA) policy for carrying out the maintenance, disposition, and access to both temporary and permanent (prior to accessioning into the National Archives) records of defunct executive agencies.

1403.2 What records and papers are not covered by this directive?
Papers and records of Presidential commissions and committees that are held by the Presidential libraries and papers and records of legislative commissions and committees that are held by the Center for Legislative Archives (LL) are not covered by this directive. These records are covered under separate governing or statutory authorities and are transferred and maintained in accordance with their legal status by the NARA custodian.

1403.3 What are the authorities for this directive?

a. 44 U.S.C 2104

b. 44 U.S.C. 2107

c. 44 U.S.C. 2108

d. 44 U.S.C. 2907

e. 44 U.S.C. 2908

f. 36 CFR 1202

g. 36 CFR 1256

h. 36 CFR 1260

1403.4 Definitions
For the purpose of this directive, the following definitions apply:

a. **Contingent record** - a record whose final disposition is dependent on an action or event, such as sale of property or destruction of a facility, which will take place at some unspecified time in the future.

b. **Permanent record** - any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States.

c. **Temporary record** - any record which has been determined by the Archivist of the United States to have insufficient value (on the basis of current standards) to warrant its preservation by NARA. This determination may take the form of a series of records designated as disposable in:

(1) an agency records disposition schedule approved by NARA (Standard Form 115, Request for Records Disposition Authority); or

(2) a General Records Schedule.

d. **Defunct executive agency** - an executive agency that has ceased to exist and has no successor in function.

e. **Executive agency** - any executive department or independent establishment in the executive branch of the Government, including any wholly-owned Government Corporation (36 CFR 1220.14).

f. **Maintenance activity** - any activity involving location of records of a Federal agency or the storage, retrieval, and handling of records kept at office file locations by or for a Federal agency (36 CFR 1220.14).

1403.5 Which agency is the successor to defunct executive agencies when there is no successor identified in the termination language?

As provided in 44 U.S.C. 2907 (operation of records centers) and 44 U.S.C. 2909 and 3303a (a) and (b) (establishment and/or revision of retention period for temporary records), the Archivist is the default successor to defunct executive agencies, and as such, the Archivist may assert legal custody over the records of a defunct executive agency.

1403.6 Who is responsible for implementing this directive?

The Archivist has delegated legal responsibility for certain activities (maintenance, disposition and access) concerning defunct agency records to the following NARA offices:

a. NARA's General Counsel (NGC) responds to access requests for records of defunct agencies that arise out of litigation; including determinations, in consultation with the office that has assumed legal responsibility of the records, of continued retention past the disposition date because of litigation (referred to at NARA as a "hold").

b. The FOIA/Privacy Act Officer (NGC) responds to access requests for defunct executive agency records, including declassification requests, from the public and other Federal agencies.

c. The Office of the Chief Records Officer (AC):

(1) identifies if there are successor agencies that continue the functions of agencies that were recently terminated, or agencies terminated after the issuance of this directive.

(2) administers the day-to-day legal responsibility (prior to accessioning into the National Archives) of defunct executive agency records.

e. The Federal Records Center Program (FRCP) maintains physical custody of the defunct executive agency records while stored in the Federal records centers.

1403.7 We are an office that has been delegated legal responsibility for records of defunct agencies. What does this mean?

As an office with legal responsibility for the records of defunct executive agencies, you have assumed the role of the original creating agency (which no longer exists). You will be responsible for maintaining the agency copy of the SF 135, Records Transmittal and Receipt, signing the disposal notices, signing the SF 258, Agreement to Transfer Records, in the accessioning process, and other functions as identified in 1403.11.

1403.8 Where will NARA store the records of defunct agencies before they are accessioned into the National Archives?

FRCs will provide storage for records of defunct executive agencies. During the time FRCs store the records of defunct executive agencies, they maintain physical custody of the records and coordinate records management activities with the NARA office that has been delegated legal responsibility.

1403.9 As an office that has been delegated legal responsibility for defunct agency records, how will we know that defunct agency records have been transferred or may already be stored at an FRC?

FRC staff will notify the offices with legal responsibility of the transfer or current storage of defunct agency records in the following manner:

a. **Initial transfer to an FRC** - If FRC staff are aware of the terminated status of an executive agency and the absence of a successor at the time of physical transfer to an FRC, or are informed of the absence of a successor after transfer, they will contact the NARA staff that will assume legal responsibility for the records. The FRC staff and the office with legal responsibility will arrange for copies of the SF 135s and/or finding aids for the records to be delivered to the office with legal responsibility.

b. **Records already stored at an FRC** - If FRC staff determines that records stored at an FRC were received from an agency that no longer exists and there are no successor agencies, the FRC staff will contact the appropriate NARA office to arrange for copies of the SF 135s and/or finding aids for the records to be delivered to the office with legal responsibility.

1403.10 I work at an FRC. How can I determine if the records are from a defunct executive agency and there is no successor agency?

If the agency has been terminated and did not provide the information to the FRC staff at the time of transfer, the FRC staff must contact AC for a determination either that the agency is defunct or that there is a successor agency.

1403.11 What activities may occur with defunct executive agency records while the records are stored in the FRCs and how will they affect us, the office with legal responsibility?

Maintenance activities (to include the initial transfer and any subsequent relocation of the records), activities that involve the disposition of the records, and activities that involve access to the records may occur while the records are stored at the FRCs. The following are maintenance and disposition activities that you may interact with FRC staff concerning defunct agency records:

a. Maintenance activities

(1) Transfer - FRC staff processes the SF 135, from the original creating agency at the time of transfer. After records are received, FRC staff forwards a copy of the SF 135 to the NARA office with legal responsibility.

(2) Relocation of defunct agency records

(a) If the records are relocated in an FRC or transshipped to another FRC, the staff of the FRC sends NA Form 13016, Notice of Transfer Location Change, to the office with legal responsibility for the records.

(b) Upon receipt of an NA Form 13016 from the FRC currently storing the records, the office with legal responsibility attaches the NA Form 13016 to the SF 135 to document the correct storage location of the records.

(3) Retrieval of defunct agency records

(a) If it is necessary to retrieve records from an FRC, the office with legal responsibility completes an Optional Form 11, Reference Request – Federal Records Center, and faxes the request to the FRC. The request should contain instructions for the delivery of the records (either a faxed copy or the original file).

(b) FRC staff retrieve the requested records and provide the requesting office with either the copies or original file.

(c) If the requesting office has requested the original file, that office returns the records to the FRC for refiling in the appropriate box.

(4) Discovery of damage to the records

(a) FRC staff contact the office with legal responsibility concerning any damage to the records that may result in the loss of information in the records; an example is detection of active mold growth on the documents.

(b) Upon notification from the FRC staff that damage has occurred to the records, the office with legal responsibility contacts Preservation Programs (RX) for

assistance is determining an appropriate treatment plan for the records.

b. Disposition activities

(1) Determination of legal holds - The office with legal responsibility implements a "hold" (an agency's temporary suspension of disposition action(s)) on the disposition of defunct agency records because of legal, audit, or investigative needs. In accordance with 36 CFR 1228.54(c)(1) through (4), the office with legal responsibility requests approval from AC for a temporary extension of retention period. The office with legal responsibility will also notify NGC of the action.

(2) Contingent records review

(a) When contingent records are scheduled for review, the FRC staff sends NA Form 13000, Agency Review for Contingent Disposal, to the office with legal responsibility.

(b) Upon receipt of NA Form 13000, the office with legal responsibility determines if the event or action has occurred that results in the final disposition of the records. If the event or action has occurred, the office with legal responsibility informs the FRC to change the disposition code and perform the scheduled disposition. If the event has not occurred, the office informs the FRC and provides a new disposition date.

(3) Disposition authority updates

(a) If records are unscheduled or require reappraisal, the office with legal responsibility completes and signs an SF 115 and submits it to AC for review. AC works with the office with legal responsibility on any issues.

(b) After a schedule is approved, AC notifies the FRCs when changes occur to the disposition authorities for defunct executive agency records.

(4) Disposal activities

(a) When temporary records have reached the end of their retention period, FRC staff sends NA Form 13001, Notice of Eligibility for Disposal, to the office with legal responsibility for the records. If the records have reached the end of their retention period; are correctly scheduled; and are not under an extended retention because of litigation ("freeze") the office signs the NA 13001 and returns it to the FRC. If the information is incorrect, the custodial office annotates the NA 13001 and returns it to the FRC without signed concurrence.

(b) Upon receipt of a signed NA 13001, FRC staff complete the disposal process according to NARA procedures.

(5) Accessioning activities

(a) In the regions, the FRCs prepare an SF 258 for those records in the regions that are eligible for accessioning into the regional archives. FRC staff forwards the SF 258 to the designated regional office with legal responsibility.

(b) In the Washington, DC, area, Archival Operations – Washington, DC (RD-DC) prepares the SF 258 for those records that are eligible for accessioning into the National Archives and forwards the SF 258 to AC.

(c) Upon receipt of an SF 258 to accession permanent records into the National Archives; the office with legal responsibility verifies that the disposition authority and retention period are correct. If the SF 258 is correct, the office with legal responsibility signs the SF 258 and returns it to the FRC. If the information is incorrect, the office with legal responsibility office must contact the creator of the SF 258 and request a revised SF 258 or schedule a new disposition date.

1403.12 Who determines if a hold on records of defunct executive agencies remains in effect?

The office with legal responsibility, in consultation with NGC, determines if a hold remains in effect on records of defunct agencies.

1403.13 How does NARA provide access to records of defunct agencies that are stored in the FRCs prior to accessioning?

Requests for access to records of defunct agencies:

a. arising out of litigation are referred to NGC.

b. (including declassification requests) from the public and other Federal agency personnel are sent to NARA's FOIA/Privacy Act Officer (NGC). NGC handles access requests as follows:

(1) First party requests, or requests from individuals for information in the records pertaining to themselves will be released in accordance with the Privacy Act. Requests from Federal agencies for information in Privacy Act systems also will be handled in accordance with the Privacy Act.

(2) Third party requests, for information in the records pertaining to another person or agency activities will be handled according to the Freedom of Information Act (FOIA).

1403.14 If we receive access requests, what fees do we charge for making copies?

Fees for copying records of defunct agencies are set in accordance with the fee schedule for accessioned records (36 CFR part 1258).

1403.15 How are records created by this directive maintained under the NARA records schedule?

a. **FRCs** maintain records created by this directive in accordance with the NARA records schedule (NARA Files Maintenance and Records Disposition Manual Records Disposition Manual [FILES 203]), items 1331 - 1334.

b. **NGC** maintains records created by this directive in accordance with the NARA records schedule items 1103-6.

c. **Offices with legal responsibility** - maintain records created by this directive in accordance with the NARA records schedule item 1312, NARA Management of Defunct Agency Records (disposition authority GRS 16, item 2).

National Archives and Records Administration

NARA 1441
September 20, 2007

SUBJECT: Appraisal Policy of the National Archives and Records Administration

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a revised policy directive that sets out the strategic framework, objectives, and guidelines that NARA will use to determine whether Federal records have archival value.

Explanation of changes. The following change is made:

- A revised entry on Observational Data in the Physical Sciences has been added to Appendix 2, Special Considerations for Selected Types of Records.

Canceled directive. NARA 1441, dated May 17, 2006, is canceled.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1441
September 20, 2007

SUBJECT: Appraisal Policy of the National Archives and Records Administration

1441.1 Purpose of this directive

a. This policy sets out the strategic framework, objectives, and guidelines that the National Archives and Records Administration (NARA) uses to determine whether Federal records have archival value. It also provides more specific guidelines for appraising certain categories of records.

b. Records appraisal is not a rote exercise. It requires informed judgments, knowledge of and sensitivity to researchers' interests, recognition of resource considerations, and a willingness to acknowledge and understand comments and suggestions from diverse perspectives. This document facilitates the appraisal process by providing a consistent framework for appraisal decision making.

1441.2 Authority for this directive

a. The authority and responsibility of the Archivist of the United States to determine the retention and disposition of Federal records stems from Chapters 21, 29, and 33 of the Federal Records Act, 44 U.S.C.

b. Chapters 21 and 29 of the Federal Records Act, 44 U.S.C. also provide for the transfer of records with archival value to NARA's legal custody when they are no longer needed for the conduct of agency business. NARA 1501, Custody of Federal Records of Archival Value sets out NARA's custody policy.

1441.3 Scope of this directive

a. All Federal governmental entities create and maintain records in the conduct of official business. However, this policy applies only to records subject to the Federal Records Act (FRA) -- records of all executive branch agencies, the United States District and Circuit Courts, and Legislative branch agencies. Records created by the President and Presidential entities, the Senate, the House of Representatives, the Architect of the Capitol, and the Supreme Court are not subject to the FRA. The appraisal of records created by these entities is not covered by this policy.

b. Certain agencies such as the Federal Deposit Insurance Corporation are not wholly governmental and are not subject to the FRA. However, these agencies typically follow FRA regulations and are covered by this policy.

1441.4 Definitions
As employed in this policy, the terms below are defined as follows:

a. **Appraisal** - the process of determining the value and thus the final disposition of Federal records, making them either temporary or permanent.

b. **Archival value -** the enduring historical or other value, as determined by the Archivist of the United States, that warrants NARA's continued preservation of records beyond the period required to transact the business of the originating agency or its successor in function. Records determined to have archival value are designated on records disposition schedules as "permanent."

c. **Intrinsic value** - archival term applied to permanent records that have qualities and characteristics that make the physical form of the record the only acceptable form for preservation.

d. **Originating agency** - the Federal agency in which records are created, received, and accumulated in the conduct of business.

e. **Permanent records** - records appraised by NARA as having archival value.

f. **Sampling** - the selection of file units or items from a body of records made in such a way that, taken together, the items selected are representative of the whole.

g. **Temporary records -** records approved by NARA for destruction after a specified event or period of time.

1441.5 Appraisal responsibilities and roles
NARA does not appraise records in isolation. As stated in its Strategic Plan, NARA works with other interested parties to ensure that "essential evidence is created, identified, appropriately scheduled, and managed for as long as needed." The Archivist of the United States has the statutory responsibility to decide how long records must be retained and which records have archival value and thus are to be retained permanently. In making appraisal decisions, the Archivist considers the recommendations of NARA staff, and seeks and considers the views expressed by originating agencies and the public.

1441.6 Strategic framework

a. NARA's mission is to ensure "for the Citizen and the Public Servant, for the President and the Congress and the Courts ready access to essential evidence."

b. Essential evidence is comprised of those records that document the:

(1) Rights of American citizens;

(2) Actions of Federal officials; and

(3) National experience.

c. Records that document the rights of citizens enable them to establish their identities, protect their rights, and claim their entitlements. Records that document actions of Federal officials that enable them to explain past decisions, form future policy, and be accountable for consequences. Records that document the national experience provide the means for evaluating the effects of Federal actions on the nation and for understanding its history, science, and culture, including the man-made and natural environment.

d. Not all records that constitute essential evidence possess archival value. Rather, NARA authorizes agencies to destroy most of these records when they are no longer needed to meet agency business needs.

e. Records that are appropriate for permanent retention are discussed below, using as a framework the definition of essential evidence spelled out in NARA's Strategic Plan.

1441.7 Permanent records categories

NARA uses the categories specified in the Strategic Plan as the beginning point for appraisal. These categories provide an overall high-level framework for the analysis of records to determine whether or not they are permanent. Note that the three categories are not mutually exclusive: some records that warrant permanent retention may fit into multiple categories, while others may relate to a single category.

a. **Records documenting the rights of citizens -** Many Federal records provide evidence of the legal status, rights, and obligations of individuals, groups, organizations, and governmental bodies. In most cases, the legal rights implications of records eventually expire. In a few instances, however, the importance of records for protecting legal rights endures despite the passage of time. Records falling into this category are preserved permanently.

b. **Records documenting the actions of Federal officials -** Most Federal records document the actions of the Government. NARA seeks to retain that portion containing significant documentation of Government activities and essential to understanding and evaluating Federal actions. For example, NARA retains permanently those records that document the basic organizational structure of Federal agencies and organizational changes over time, policies and procedures that pertain to an agency's core mission, and key agency decisions and actions.

c. **Records documenting the national experience -** Some records document the impact of Federal actions on individuals, communities, or the natural and man-made environment. The Government also creates and acquires much information about people, places, material objects, and scientific phenomena, as well as about social conditions, political and economic activities, and events in the United States and other countries. Much of this information does not have archival value. However, some is essential to understanding the role of the Federal Government and the history of our nation, its people, and the environment.

1441.8 Appraisal objectives

Within the high-level strategic framework of rights, actions of Federal officials, and the national experience outlined above, NARA will identify for permanent retention records that:

a. Retain their importance for documenting legal status, rights and obligations of individuals, groups, organizations, and governmental bodies despite the passage of time;

b. Provide evidence of significant policy formulation and business processes of the Government;

c. Provide evidence of our Government's conduct of foreign relations and national defense;

d. Provide evidence of Federal deliberations, decisions, and actions relating to major social, economic, and environmental issues;

e. Provide evidence of the significant effects of Federal programs and actions on individuals, communities, and the natural and man-made environment;

f. Contribute substantially to knowledge and understanding of the people and communities of our nation.

1441.9 General and specific guidelines

NARA uses the general guidelines outlined in appendix 1 to determine which records support its appraisal objectives and thus warrant permanent retention. NARA has also developed specific appraisal guidelines for selected kinds of records (see appendix 2). Permanently valuable records sometimes have qualities and characteristics that make the records in their original physical form the only archivally acceptable form for preservation. The qualities and characteristics of records with intrinsic value are outlined in appendix 3.

1441.10 Reappraisal

NARA will reappraise records when there is compelling evidence that earlier appraisal decisions require review. In such circumstances, NARA will seek Federal agency and public involvement in the reappraisal process.

1441.11 Policy review

NARA will review this policy as necessary in consultation with Federal agencies, research communities, and other interested parties.

1441.12 How are records created by this directive maintained under the NARA records schedule?

Maintain records created by this directive in accordance with the NARA records schedule (NARA Files Maintenance and Records Disposition Manual Records Disposition Manual [FILES 203]), items 1307 – 1311.

Appendix 1 - General appraisal guidelines

In appraising records to decide whether records have archival value and should be retained permanently, NARA will use the guidelines found below. Applying the guidelines to specific cases will not be a mechanical process akin to adding up points or checking boxes. However, using these guidelines will make decision making easier and will result in more consistent appraisal judgments that can be readily explained both within NARA and to outside constituents. In developing appraisal recommendations for the Archivist of the United States, NARA staff must address the following questions. The questions should be considered together, rather than in isolation.

How significant are the records for research?
The future research potential of records is the most difficult variable to determine. What is of relatively low research use today may become of great research use in the future. Perhaps even more important and difficult to predict are the issues and topics that will be considered of significance in the future. Nevertheless, it is important to consider this question in making appraisal decisions. It is necessary to consider the kinds and extent of current research use and to try to make inferences about anticipated use both by the public and by the Government.

How significant is the source and context of the records?
The significance of the functions and activities performed by the originating agency or agencies and the business context within which the records are created are important considerations for the appraiser. The appraiser must relate the source and context of the records to the strategic framework and objectives found in this directive.

Is the information unique?
Appraisals must be conducted in context with other records. The appraiser must determine whether the records under consideration are the only or most complete source for significant information. Records that contain information not available in other records (including other Federal records as well as files accumulated by state and local governments) are more likely to warrant permanent retention than records containing data that is duplicated in other sources. However, NARA may decide to retain records that contain information available elsewhere in the case of records that are more complete or more easily accessible than the alternative source.

How usable are the records?
Consider these three issues:

1. **How does the way records were gathered, organized, presented, or used in the course of business affect their usability?** For example, records whose arrangement, indexing, or other identifying information makes it easy to locate needed information are more likely to warrant retention than records containing similar documentation that are extremely difficult to use.

2. **How do technical considerations affect the usability of the records?** For example, some electronic records may pose such technological challenges that extraordinary measures may be required to recover the information, while other records containing

similar documentation (either electronic records or records in another format) may be usable with much less effort.

3. **How does the physical condition of the records affect their usability?** For example, some records may have deteriorated to the point that the information they contain is not readable.

Do these records serve as a finding aid to other permanent records?
Records that can be used as a finding aid to other records may warrant retention even if the information they contain is not unique or complete. For example, the records may enable a researcher to identify which state or local government holds birth certificates, marriage licenses, and other documents relevant to his or her research.

What is the timeframe covered by the information?
"Timeframe" may refer to the date span of the entire body of records or the length of time that individual records or file units typically cover.

1. The longer the date span for which there are extant files, the more valuable the records are likely to be for research. For example, they might be valuable to support longitudinal studies by the Government or other researchers.

2. Some bodies of records are made up of individual documents or files whose content covers many years. This attribute includes records where the documents in individual files are accumulated over a relatively short period but contain information pertaining to events covering a long period of time (e.g., official military personnel folders or military unit histories).

Do the records document decisions that set precedents?
Do decisions or actions of the originating agency set precedents, or is each decision or action independent of others and merely based on policy set at some higher level? If the former, the records are more likely to warrant permanent retention. Examples include appellate court decisions and policy files at the highest level within an agency.

Are the records related to other permanent records?
Other things being equal, records that add significantly to the meaning or value of other records already appraised as permanent are more likely to warrant retention than records lacking such a relationship. Records that are chronological continuations of records already in the National Archives are likely to warrant permanent retention, particularly if the older segments of the records are subject to high reference use.

Do the files contain non-archival records?
Files that contain only a small interspersion of records lacking archival value (i.e., non-archival records), such as routine fiscal documents, records relating to the issuance of expendable supplies, etc. are more likely to be appraised as permanent than records where the interspersion of non-archival documents is high, particularly if the overall volume of the records is large. When the volume of records containing some highly valuable material is relatively small, it may still be appropriate to appraise the records for permanent retention even if a significant fraction

of the records lack archival value. Disposition instructions should allow (but not require) NARA to dispose of non-archival records after the originating agency transfers the records to NARA's legal custody.

What are the cost considerations for long-term maintenance of the records?
This consideration should play a significant role only in marginal cases. In such cases, an appraisal should balance the anticipated research potential of the records with the resource implications of retaining them permanently. Other things being equal, records with low long-term cost implications are more likely to warrant permanent retention than those records that carry high long-term costs.

What is the volume of records?
Propose for permanent retention (regardless of volume) records that are clearly permanent in accordance with other appraisal guidelines. Volume will play a role only in the appraisal of records whose archival value is marginal. Other things being equal, records that are compact are more likely to be appraised as permanent than those that are voluminous.

Is sampling an appropriate appraisal tool?
Appraisal decisions that call for sampling records may be made only after careful analysis of all other options and the costs and benefits of implementing a sampling decision. A sampling disposition will not be used where this option merely defers problems. Wherever possible, a sampling disposition should be avoided where the disposition requires item by item decisions to retain individual records or individual file units.

Appraisal decisions involving sampling must specify a process that permits the easy identification of records that are to be retained permanently.

- Processes that involve subjective judgments or item by item decisions to retain individual records or individual file units require a justification detailing the circumstances that prevent an objective, easily implemented process and estimating the staff hours required to perform the sampling on a year's accumulation of records.

- Appraisal decisions involving sampling must specify whether the originating agency or NARA will be responsible for implementing the sampling work.

- Where the need for sampling is driven by the originating agency, this appraisal decision should only be made if the agency is strongly committed to doing the sampling work.

- Where the need for sampling is driven by NARA staff, this appraisal decision should only be made if NARA archival personnel are strongly committed to doing the sampling work and have the resources to do it.

Appendix 2 - Special considerations for selected types of records

Some types of records require special consideration in the appraisal process. The appraisal factors identified in this appendix will be used together with the general guidelines in Appendix 1 and the strategic framework and objectives found in the main body of this policy document. This appendix will be expanded if guidelines for additional types of records are developed.

PERSONAL DATA

Personal data records contain information about an individual and may also include information about his or her family members. Included are such records as the personnel folders of Federal employees and members of the armed services; the files that are accumulated in connection with determining an individual's eligibility for Federal Government benefits, such as a pension, medical care, or mortgage guaranty; and the records that document the immigration to the United States of the foreign born or their application for legal residence or citizenship.

In appraising personal data records, it is necessary to take into account the following:

- **Size and nature of the population**

Some personal data records cover nearly all of the American population. Records of this sort are more likely to warrant permanent retention than records containing information on only a small percentage of the population. However, even if the total number of people represented in a body of personal data records is relatively low, the records may still warrant permanent retention if they contain information concerning a large percentage of a subgroup of the American population (e.g., an ethnic or racial group or residents of a specific region).

- **Nature of the information**

Researchers who use personal data records have traditionally had a high interest in the following types of information concerning individuals. Records that are rich in the kinds of information outlined below are more likely to warrant permanent retention than records that contain only a small number of these elements:

  - previously used names
  - date and place of birth, place(s)of residence;
  - date, place, and cause of death;
  - if foreign-born, date and place of arrival in the US, and if naturalized, date and place of naturalization;
  - names of parents;
  - dates and places of parents' births and deaths;
  - name(s) of spouse(s), date(s)and place(s)of marriage;
  - names of children;
  - date and place of children's birth;
  - education level;
  - educational institutions attended and the dates;

- occupation;
- property ownership;
- names of employers and work location(s)
- military service, including branch of service, dates of service, and rank
- identification photographs of individuals

Researchers appear to be increasingly interested in medical information as well. NOTE: It will be necessary to monitor possible effects of the Health Insurance Portability and Accountability Act (HIPAA) on access to medical information.

OBSERVATIONAL DATA IN THE PHYSICAL SCIENCES

The physical sciences encompass any of the sciences that analyze the nature and properties of energy and nonliving matter (thereby excluding the biological sciences and social sciences). The physical sciences include chemistry, physics, the space sciences (astronomy, planetary science, and space physics), and a number of earth sciences (including geology, hydrology, meteorology, oceanography, and soil science). These disciplines often are overlapping, as illustrated by space physics, chemical physics, physical chemistry, and geophysics.

While some of the physical sciences (including chemistry and materials sciences) produce experimental data, many of them (including the space sciences and earth sciences) collect data on the observation of natural phenomena. Observational data characteristically are unique and non-repeatable and can be generated in large volumes.

Federal agencies follow a standard work process for developing and using observational data. The steps in this process are collecting, processing, and interpreting data; preparing related products; and documenting, storing, cataloging, and managing data and products to make them available for continuing use.

Raw observational data are collected by means of human perception or measurement (e.g., field notes) or, more commonly, by sensor or other instrument. *In situ* data collection is carried out in direct contact with the phenomenon under study. Examples of *in situ* sensors are stream flow gauges, seismic gauges, and sensor packages mounted on buoys. By contrast, remote sensing involves use of instruments, such as cameras or digital sensors, not in close contact with the studied phenomenon.

Data may be collected in any location – the earth, the atmosphere, or in space. In recent decades, data usually have been collected in digital formats, although in the past they commonly were collected in analog formats, such as paper or photographs, a portion of which may not have been converted to digital format.

After collecting raw data, scientists process them at different levels of complexity. Each processing level provides added value through such actions as summarizing and interpreting the raw data and synthesizing new data. Production of processed data may involve incorporating two or more sources, raw or processed, to generate yet another data product, for example, the merging of observational and elevation data to produce three-dimensional representations. Processed data frequently are subjected to scientific peer review. A dataset consists of a body of

related data (raw and/or processed), for example, data gathered from a particular satellite sensor for a given time period and geographic region.

Data originators are responsible for documenting their data, including preparation of metadata (i.e., the auxiliary information needed to understand and use data properly). Data originators also are generally responsible for submitting their data and metadata to a data center for long-term storage. Such centers catalog the data and make them available for continuing use, often by posting the data or linkages to the data on appropriate websites.

Primary use of observational data is usually by scientists involved in collecting and initially processing the data. Secondary use of data is by others than those involved in collection and initial processing. Secondary users include scientists and non-scientists. Scientists often exploit the data in new ways and, in so doing, may create additional processed datasets. Non-scientists use data in a variety of ways. For example, farmers use climatological data for decisions on crop selection, and engineers use seismic data in designing critical structures such as nuclear power plants.

Primary or secondary use of data can result in preparation and dissemination of related products – either processed data or non-data products. Examples of non-data products are (1) hurricane warnings and weather forecasts prepared from meteorological data, (2) navigation charts and maps prepared from oceanographic data, and (3) maps of flood-prone areas prepared from hydrologic data. Certain products are produced by running data through a model (software using mathematical formulas) used to simulate natural phenomena. Such models may generate, for example, products used to forecast the weather or the progress of a wildfire.

Agencies holding large quantities of observational data include the National Oceanic and Atmospheric Administration (NOAA), National Aeronautics and Space Administration (NASA), and U.S. Geological Survey (USGS). These agencies both collect data themselves and receive data submitted by outside entities. The agencies maintain *in situ* and remotely sensed data pertaining primarily to space and the global environment, including the atmosphere, ocean, and land surface. These data are stored, cataloged, and distributed by multiple data centers. The observations not only support real-time monitoring and forecasting but over time provide a historical record.

Appraisal considerations:

- Appraisal of observational data is challenging because appraisers frequently must deal with a high volume of data and become familiar with a diversity of data structures and platforms, metadata requirements, and media types including paper, audio-visual, and electronic.

- Observational data are likely to be appraised as either long-term temporary or permanent. Unlike laboratory experimental data, observational data typically document phenomena that can never be repeated. Observational data establish a baseline to help determine future rates of change and frequency of occurrence of unusual events. Moreover, observational data frequently can be processed and used in novel ways, for example, to verify new scientific concepts.

- Observational data covering a long time period tend to have more value because they enable long-term patterns to be identified and thereby increase confidence in the reliability of data and the conclusions drawn from them. In addition, data are more likely to be appraised as permanent if they not only can be used for scientific purposes but also for legal, commercial, educational, engineering, resource management, or other purposes.

- Appraisal decisions should take into account that the uses of data vary according to the level of processing. Raw or minimally processed data are more difficult for anyone except the primary user(s) to understand and use but are essential for conducting a reanalysis, such as to verify findings or support a new hypothesis. With each higher level of processing, data generally become easier to use but less subject to reanalysis. To facilitate future reanalysis, it is usually appropriate to preserve processed data at the lowest level of processing compatible with effective use. Processed data are more likely to have long-term value if they would be costly to recreate from the raw data. It may be warranted to appraise as permanent both a raw version and one or more processed versions of certain data.

- To be appropriate for long-term temporary or permanent retention, observational data should possess authenticity, reliability, integrity, and usability (as defined in ISO 15489-1). Intellectual linkage with the related metadata is essential, and linkage with program or project management records is desirable to provide additional context for the data.

- Additional factors favoring long-term or permanent retention are uniqueness, completeness, and quality of observational data; quality and completeness of metadata; and availability of appropriate technology to enable access. In general, data are more likely to have these attributes if the data have successfully undergone the scientific peer review process. Distributed storage of data does not diminish their archival value, provided that a central catalog is maintained to ensure access.

- Metadata should include information such as purpose and time period of data collection; location of collection site; methods and instrumentation used in collection; units of measurement, acceptable values, and error tolerance; data aggregation methods; processing history; and quality assessment. The types of metadata required vary with the nature of the data and their likely future uses. It is preferable for metadata, whenever possible, to conform to standards issued by such broad-based organizations as the Federal Geographic Data Committee (FGDC) and the International Organization for Standardization (ISO).

- It is appropriate for many observational data of long-term temporary or permanent value to be maintained on a continuing basis by a scientific data center that possesses the necessary expertise to ensure preservation and access. Data centers often issue policies on collecting and data sharing. NARA appraisers will benefit from reviewing these policies and identifying the standards used to determine which data have value for long-term scientific purposes. Similarly, appraisers should seek the advice of scientists when assessing many of the above-mentioned attributes of data and metadata.

- Many data series now collected in electronic format were formerly created and maintained in other formats such as paper or photographs. Agencies may still maintain older data in such formats for use in conjunction with the related electronic data. Appraisers should extend their

review of electronic systems to include any related data in other formats, as these older data may add to the usefulness of the electronic data if they are still in a usable format. All formats should be considered during the appraisal.

- Models are rarely if ever appropriate for appraisal as permanent. Models generally are in a continuous state of development, so that one model will replace another as soon as its value is demonstrated (e.g., improved accuracy in forecasting hydrologic conditions). Data products that result from running data through a model may warrant permanent retention if they relate to a significant phenomenon or occurrence.

ENVIRONMENTAL HEALTH AND SAFETY RECORDS

This section covers environmental health and safety (EH&S) records relating to Federal actions in regard to hazardous substances and their potential harmful effects on humans and the environment. The types of hazardous substances are diverse and include radioactive substances, asbestos, certain metals such as lead and mercury, synthetic chemicals (such as PCBs), petroleum products, and munitions. Not covered here are records relating to the following types of environmental health and safety hazards: communicable disease agents, fires and natural disasters, and hazards from use of tools and equipment.

Federal government agencies undertake several broad functions that generate a wide variety of EH&S records. The first is production, use, storage, transportation, and disposal of hazardous substances. The second consists of planning and routine monitoring of actions involving potential release of hazardous materials into the environment and exposure of people to them. Planning includes preparation of environmental impact statements (EISs) and similar documents.

A third EH&S function involves emergency response, monitoring, and remediation of spills and other inadvertent or unauthorized releases. These actions may involve either short-term, prompt removal of hazardous substances or long-term remedial response. Monitoring may be included in either the second or third above-mentioned EH&S function and generally consists of data collection, analysis, and documentation of releases and exposure involving hazardous substances. A fourth EH&S function relates to conducting litigation and responding to claims relating to potential harm caused by hazardous substances to individuals and the environment. The third and fourth EH&S functions may relate to substances not known to be hazardous at the time of production, use, or disposal.

Numerous environmental laws establish requirements, including those for recordkeeping, in regard to hazardous substances. Many of these laws require Federal agencies to comply with general environmental standards for production, use, and disposal of hazardous substances, as well as for environmental planning and routine monitoring. An example is the National Environmental Policy Act (NEPA), which mandates that agencies formally analyze the environmental consequences of a proposed major action and consider possible alternatives.

Environmental laws give certain agencies jurisdiction over emergency response and cleanup involving significant releases, spills, and waste sites, including those not caused by the Federal government. These laws set strict requirements for financial oversight and involvement of the public in regard to response and cleanup.

The most important of such laws are the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) and its reauthorizing legislation, the Superfund Amendments and Reauthorization Act (SARA). CERCLA and SARA give the Environmental Protection Agency (EPA) overall authority for most major environmental remediation and establish the Superfund to support this remediation. Under the aegis of these and similar laws, national defense agencies perform cleanup of former military sites in conformance with the Defense Base Closure and Realignment Act of 1990 (BRAC), Formerly Used Defense Sites (FUDS) program, and similar programs.

In addition, the Oil Pollution Act (OPA) gives certain agencies, such as the National Oceanic and Atmospheric Administration, authority for response and remediation for major oil spills. Lastly, a number of Federal laws provide for financial compensation to certain workers and other individuals exposed to hazardous substances.

Appraisal considerations:

- The National Environmental Policy Act (NEPA) requires Federal agencies to prepare environmental impact statements (EISs) for major Federal actions that significantly affect the quality of the environment. An EIS is a full disclosure document that details the process through which a project was developed, considers a range of reasonable alternatives, analyzes the potential impacts resulting from the alternatives, and demonstrates compliance with other applicable environmental laws and executive orders. The EPA collects and maintains a record set of agency environmental impact statements (EISs). These EISs, which are scheduled for permanent retention, provide important evidence of agency decision-making and the condition of the environment before actions are taken.

- Copies of EISs held by the creating agencies usually are scheduled as temporary. Other agency environmental planning records, such as environmental assessments and categorical exclusions, also tend to be scheduled as temporary because they document environmental decisions of lesser magnitude than those covered by EISs. Long-term temporary retention may be appropriate for agency EISs and related planning records due to their legal importance in documenting environmental changes.

- A number of agencies involved in major environmental remediation actions are required to maintain an Administrative Record (AR) documenting the decision-making process and public participation in the remediation. An AR is the complete body of documents that forms the basis for selecting a response action (i.e., documents considered or relied upon in selecting a remedy). The AR and other major remedial records frequently are appraised as permanent because they help document both significant environmental damage and proposed restoration activities. Such records are likely to have particular value for local history, because they describe and measure the consequences of damage to communities, their local economies, and their immediate environment.

- Fiscal and administrative records accumulated during cleanup and restoration tend to have long term temporary retentions. The process of assessing damage and implementing restoration can take years, and the associated costs charged to parties responsible for the

damage can be considerable. Retention periods of thirty years beyond case closure or restoration completion are frequently applied to contracts and accounting and financial records that ordinarily would have much shorter retentions if covered by the General Records Schedules.

- Records documenting the Federal Government's disposal of individual pieces of real property often have permanent value, because such records may document the condition of the site at the end of a particular phase of operations, prior to change of ownership.

- Irreproducible data supporting epidemiological studies or other significant analyses of exposure of humans and the environment to chemicals, pesticides, and hazardous wastes may have sufficient value to warrant permanent retention, depending on the breadth and scope of the analysis and the reusability of the data.

- Data that track or model long-term exposure conditions and responses at abandoned, inactive, or uncontrolled waste sites and the releases of hazardous wastes may also have sufficient value for permanent retention, depending upon the general public or research community interest in the site or release and the purpose for which the data was collected. Although programs marginally involved with high profile events and sites often keep considerable amounts of related data, the data documenting the activities and/or programs having responsibilities directly associated with the event or site are the most likely to have permanent value.

- Claims files relating to health and safety issues are generally disposable in either electronic or hardcopy form, though they may have lengthy retention periods. Information systems for managing claims files, however, may be permanent, as the data can be manipulated and may have value for documenting the number and types of cases, as well as their handling and disposition.

- Photographs, films, videos, and other audio-visual records relating to the production, use, and disposal of hazardous substances often are of permanent value, because they help document such matters as work processes, working conditions, and layout of hazardous waste sites.

- Other records concerning the production, use and proper disposal of hazardous substances are usually appraised as temporary. Examples of such records are manufacturing or construction project files, Material Safety Data Sheets, calibration records, inventory and inspection records, shipping manifests, chain of custody documents, and certificates of disposal. Some of these records have lengthy temporary retentions to protect the rights and interests of individuals, organizations, and the government in regard to the potential long-term harm caused by hazardous materials. The longest retentions generally are provided for records relating to radioactive material, because of its ongoing potential for harm. Also, records and data resulting from routine monitoring of individuals' exposure to hazardous substances generally have long-term temporary retentions to protect rights and interests.

- Records and data relating to production, use, disposal, and routine monitoring of hazardous substances may be subject to an agency-imposed disposition moratorium because of their long-term utility for litigation, environmental investigations, and epidemiological studies.

Such a moratorium generally does not mean that the records and data are appropriate for permanent retention.

- When Federal law or regulation specifies a minimum retention period for particular EH&S records, it usually is appropriate to schedule retention for that minimum period. However, longer retention may be necessary when an agency has special legal or business requirements for the records, and permanent retention may even be warranted in rare circumstances.

RESEARCH AND DEVELOPMENT (R&D) RECORDS

This section discusses research and development (R&D) records relating to the planning and execution of basic and applied research in engineering and the physical and natural sciences. Basic research seeks to generate new knowledge, and applied research uses the results of basic research and applies them to the design, development, and testing of new products and processes. Agency R&D programs tend to be large in scale, expending hundreds of millions of dollars annually and generating voluminous records. Records pertain to such research fields as biology, chemistry, medicine, physics, materials science, aerospace technology, weapons development, computer science, energy development, and environmental protection.

Appraisal of the records requires an understanding of the entire R&D business process, including the project/product lifecycle and use of outside entities for review or support. Most R&D conducted by or for the Federal government follows a standard workflow based on the scientific method. The basic steps include formulating a hypothesis or statement of need, obtaining approval and/or funding, designing and conducting experiments and analyzing results, and disseminating findings. Records created and accumulated by these steps can be separated into the following categories: program management records covering the processes of formulation, selection, and funding; project records covering design, collection, analysis, and reporting; and dissemination of findings. Types of records found under these categories include planning records, project files, procurement and financial records, laboratory notebooks, research data, and technical reports and similar publications.

The status and availability of records produced by a project often depend upon the funding arrangement. For projects funded by contracts, records specified in the contract as deliverables generally are Federal records and, in conformance with the contract requirements, may be maintained by either the contractor or the funding agency. By contrast, the primary records of grant-funded projects usually are not considered to be Federal records and are maintained by the grantee. Recordkeeping for collaborative projects is affected by the diversity of funding sources and institutions (including non-Federal institutions) involved. Effective appraisal of these records requires a determination of which institutions have responsibility for the records and their disposition.

Appraisal considerations:

- Program management records that document the planning, policies, and priorities of research programs usually are appraised as permanent. Such records may be maintained by offices with agency-wide R&D responsibilities, by individual divisions and laboratories, and by

scientific and technical advisory bodies. Using the guidance in appendix 1 – General Appraisal Guidelines, appraisers should determine for which office(s) within a given agency these records should be scheduled as permanent.

- Technical reports, conference proceedings, and similar publications that disseminate the findings, methodology, and conclusions of projects are usually appraised as permanent and are often maintained centrally by an agency component responsible for their collection, management, and distribution. Review of a cross-section of such publications can help determine the subject matter and scope of R&D projects and thereby prove useful in assessing the value of other project-related records and data.

- Project files may include such records as statements of work, progress reports, briefing papers and presentations, specifications and drawings, laboratory notebooks, research data, environmental and safety information, and technical reports. Agencies may maintain such files as case files or as separate series. The value of project files varies across R&D programs, based on such factors as the files' organization and content, nature and scope of the research, and extent to which separately maintained series of records such as annual reports, planning records and technical reports provide sufficient documentation of the projects.

- Because many R&D projects have a very limited focus and project records often are voluminous, a very strong justification is needed to appraise all of an agency's project files as permanent. If selection criteria are to be applied to identify files for permanent retention, the creating agency or organization must devise a practical arrangement for applying the criteria to the records and agree to implement it, because it is the creating agency which possesses the expertise and resources to evaluate the files individually. For overall guidance on when to apply selection criteria, see appendix 1 – General Appraisal Guidelines – "Is sampling an appropriate appraisal tool?"

- Contracting, procurement and other fiscal records generally are appraised as temporary when readily segregable from other project records.

- Laboratory notebooks may be informally maintained as part of project files, or as a separate series, issued formally and strictly controlled to protect intellectual property and patent rights. Notebooks issued and managed formally are more likely to be appraised as having long-term temporary value or possibly permanent value.

- Research data created by R&D projects may be unprocessed (raw) or processed (compiled or analyzed) at different levels. Raw data are generated by an experiment, whereas processed data consist of raw data manipulated to help identify patterns in the data. It is very difficult to generalize about the value of processed data as opposed to raw data, as both have their own significance for the research process. Research data most often are electronic but also may be in another format such as paper or photographs. To help establish the value of still photographs and moving images, whether conventional or digital, maintained separately from other project records, appraisers need to determine whether the agency maintains intellectual linkage between these and related project records.

- Research data commonly have short-term value when they are narrow in scope and can be

replicated by a new experiment if necessary. Data may have long-term temporary or even permanent value when they are extremely difficult or impossible to replicate and are potentially useful for such purposes as permitting an important experiment to be reviewed and validated, supporting new scientific research, or providing a legal basis for health-related claims.

- For data to be valuable over the long term, they should be unique, complete, valid, and accompanied by appropriate metadata. Moreover, data are usually more valuable when they can be linked to records describing the research protocol and modes of analysis. In considering these qualities of data, appraisers should consult with the relevant scientific experts. Data with long-term research value often are most appropriately maintained by the R&D agencies which created them because the creating agencies usually possess the scientific expertise essential for providing effective access to the data.

- R&D agencies, particularly those involved in environmental or health research, may create tissue samples, slides, and specimens which are treated by researchers as project records and preserved by the agency for long periods at substantial expense. Although NARA generally does not consider such materials to meet the definition of Federal records, agencies nonetheless need to manage them properly because of their importance to R&D programs and potential for long-term use.

Appendix 3 – Qualities and characteristics of records with intrinsic value

Documentary materials, regardless of origin, having intrinsic value are rare and possess one or more of the following specific qualities or characteristics. These qualities and characteristics relate to the physical nature of the records, their prospective uses, and the information they contain. NARA will use the guidelines below in deciding whether permanent records have intrinsic value and should be retained in their original form.

1. *Physical form that may be the subject for study if the records provide meaningful documentation or significant examples of the form*

   Documents may be preserved in their original form as evidence of technological development. For example, a series of early press copies, glass-plate negatives, or wax-cylinder sound recordings may be retained. All records having a particular physical form would not be considered to have intrinsic value because of this characteristic; however, a selection broad enough to provide evidence of technological development would be considered to have some value. Determination of intrinsic value based on a particular technology would be rare since it would be preserving a particular form for its value as an artifact rather than for archival value.
2. *Aesthetic or artistic quality*

   Records having aesthetic or artistic quality may include manuscripts; photographs; pencil, ink, or watercolor sketches; maps; architectural drawings; frakturs; and engraved or printed forms, such as bounty-land warrants.
3. *Unique, curious, or historical physical features or formats*

   Physical features that are unique, curious, or historically significant might include quality; texture of paper; color; wax seals; imprints and watermarks; inks; and early or unusual bindings. All records having a particular physical feature would not be considered to have intrinsic value because of this feature; however, a representative selection of each type would be considered to have such value.
4. *Age provides a quality of uniqueness*

   Age is a relative rather than an absolute quality. Generally, records of earlier date are of more significance than records of later date. This can be because of a historical change in the functions and activities of the creator of the records, the scarcity of earlier records, a change in recordkeeping practices, or a combination of these.
5. *Value for use in exhibits*

   Records used frequently for exhibits normally have several qualities and characteristics that give them intrinsic value. Records with exhibit value impressively convey the immediacy of an event, depict a significant issue, or impart a sense of the person who is the subject or originator of the record. In these cases, the impact of the original document cannot be equaled by a copy.
6. *Questionable authenticity, date, author, or other characteristic that is significant and ascertainable by physical examination*

   Some records are of doubtful authenticity or have informational content that is open to question. Although it is impossible to foresee which documents will be questioned in the future, certain types of documents are well known to have the potential for controversy and, if the original records are extant, handwriting and signatures can be examined, paper

age can be ascertained, and other physical tests can be performed. In some cases the controversy can be resolved by recourse to the original item (such as by examination of the handwriting, the age of the paper, or the original negative of the photo static print), while in other cases the item will not be conclusive but will provide the researcher with the best evidence from which to draw conclusions (original photographs of unidentified flying objects, for example).

National Archives and Records Administration

NARA 1462
September 28, 2006

SUBJECT: Recovery of Alienated Archival Materials

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Incorporating Change 1, April 9, 2013

Purpose of this transmittal memo. This transmits a revised directive that outlines NARA's policy on replevin and criteria that staff must use to act on allegations and instances of alienation of archival materials that were in the National Archives of the United States or that should have been in the National Archives of the United States.

Why are we revising this directive? This directive, first issued on March 27, 2003 as Replevin of Archival Materials, now includes updated guidance to inform staff of instances when NARA may decide to pursue custody of Federal records that were never accessioned into the National Archives of the United States.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

NARA 1462
September 28, 2006

SUBJECT: Recovery of Alienated Archival Materials

1462.1 What is the purpose of this directive?
This directive specifies NARA's policy on replevin and the procedures for acting on allegations and instances of alienation of archival materials that were in the National Archives of the United States or should have been in the National Archives of the United States.

1462.2 What is the authority for this directive?

a. 44 U.S.C. 2107, 44 U.S.C. 2111, 44 U.S.C. 2111note, 44 U.S.C. 2112, 44 U.S.C. 2202, and 44 U.S.C. 2207 authorize the Archivist of the United States to accept records with historical value from Federal agencies, Congress and legislative branch agencies, the judiciary, and Presidential administrations.

b. As the lawful custodian of archival Federal and Presidential records, the Archivist is also authorized under 44 U.S.C. 2905(a) and 44 U.S.C. 3106 to pursue replevin actions to recover records alienated from Federal custody that were or should have been in NARA's custody.

c. The Inspector General Act of 1978, as amended, 5 U.S.C. App. 3 also applies.

1462.3 Definitions

a. **Alienation** is: In a strict legal sense, the transfer of ownership of property. In addition, as used in this directive, **alienation** is the improper transfer or loss of custody of records/archives by their original custodian or owner to someone not legally entitled to them.

b. **Owner** is the individual or entity having legal title to records or archives. In this directive **owner** does not refer to an individual or entity having only physical possession of records or archives.

c. **Replevin** is the term used to describe a legal mechanism by which an owner recovers property that has been improperly separated or illegally removed from its custody. For purposes of this directive, this refers to NARA's civil recovery of archival materials.

1462.4 What materials are covered by this directive?
This directive covers archival Federal records, Presidential and Vice Presidential records, Nixon Presidential historical materials, and donated historical materials, including artifacts, that were or should have been in NARA's custody.

1462.5 What records are not covered by this directive?
This directive does not address:

a. Records held by a Federal agency that are eligible for immediate accessioning into the National Archives (sometimes referred to as "retained records").

b. Records improperly removed from an agency when the records are still in the legal custody of the agency. (See NARA 1463, Unauthorized Destruction or Removal of Federal Records at Agencies, for steps NARA takes to assist agencies with the recovery of records removed while still in their legal custody.)

c. Loans of records in the National Archives to Federal agencies and other institutions. (See NARA 1701, Loans of Holdings in NARA's Physical and Legal Custody, for issues relating to securing overdue loans of records.)

1462.6 Who is responsible for implementing this directive?

a. All NARA staff are responsible for reporting the discovery of suspected alienated records to their immediate supervisor and the Office of Inspector General (OIG). Par. 1462.7 describes the procedures to follow.

b. The pertinent custodial unit in Legislative Archives, Presidential Libraries, and Museum Services (L) or Research Services (R) reviews the records in relation to NARA's holdings and provides supporting information to OIG and NGC, as appropriate.

c. The Office of the Inspector General (OIG) investigates suspected criminal alienation and seeks recovery of archival materials that have been removed from NARA's custody. OIG:

(1) Notifies the Archivist, General Counsel (NGC), and the appropriate office of any reports as appropriate;

(2) Uses investigative methods permissible under the Inspector General Act of 1978 (Pub. L. 95-452), as amended, such as subpoena power, interviews, or other means;

(3) Works with individuals or entities contacting NARA about possible lost and stolen documents, as a result of the appeals on *www.archives.gov*, partnership with outside organizations, or other means;

(4) Mobilizes the Archival Recovery Team, which consults with NARA subject matter experts and NGC; and

(5) Consults with the Department of Justice (DOJ) as appropriate.

d. The Office of General Counsel (NGC) handles NARA's civil recovery efforts through settlement, replevin litigation, or other legal means. NGC:

(1) Notifies the Archivist, OIG, and the appropriate NARA office (if the report did not come from the office) of any reports relating to suspected alienation;

(2) Develops the necessary background information about the records with the assistance of the relevant NARA custodial unit(s);

(3) Coordinates with DOJ, as appropriate, if NARA seeks civil remedies; and

(4) Obtains the approval of the Archivist before engaging in any recovery action.

1462.7 What must be done if alienation of records is suspected?

a. Any staff member who discovers or receives a report of suspected alienated records (including information received in good faith from an institution that discovers possible alienated records among its holdings) must notify his or her immediate supervisor and OIG. See the Recovery Flowchart at the end of this directive.

b. If suspected alienated records are to be auctioned or otherwise sold, provide OIG and NGC sufficient information to evaluate whether to try to stop the sale, while more detailed information is being developed (see subpar. e).

c. The pertinent custodial unit in L or R conducts an initial assessment and reports to OIG as quickly as possible on whether the item:

(1) Is a Federal record;

(2) Is appropriate for preservation at NARA; and,

(3) Was ever in the possession of NARA.

d. If all three conditions are met, the OIG has lead responsibility. If conditions one and two, but not three, are met, then NGC has the lead responsibility.

e. The custodial unit of the records then works with OIG and NGC as appropriate on the investigation and recovery effort, including by providing the following information:

(1) A clear description of the records, including date span and subject matter if possible,

(2) A copy of the information that brought the records to the staff member's attention (e.g., catalog page, a letter from the public, or if an online auction, cite the specific item control number or other identifier).

(3) Contact information for the current holder of the records, including the name of individual or institution, address, phone number, and relevant web sites or e-mail addresses, if known; and, if possible,

(4) For records that were held by NARA, documentation establishing that the records had been in NARA's physical or legal custody, such as a NARA-signed Standard Form 258, Agreement to Transfer Records to the National Archives of the United States, signed deed of gift or deposit agreement, Transfer Request or Legal Transfer Instrument from ERA, or other legal documentation. Examples of other evidence are that the records are reproduced in a microfilm publication or described in a guide to records, finding aid, or other NARA product. A Federal file code or equivalent marking on documents is also another useful indicator. If such documentation is not immediately available, forward it as soon as it is located to OIG in a follow-up to the first notification of suspected alienation.

f. In the case of a possible violation of an affiliated archives agreement:

(1) Staff must notify their immediate supervisor who must notify the Affiliated Archives contact and the R Access Coordinator who monitors the specific Affiliated Archives involved in the possible violation; and

(2) The Access Coordinator may request that NGC review the relevant affiliated archives agreement and advise on the possible violation.

~~(1) Staff must notify their immediate supervisor who must notify the Affiliated Archives contact and the R Affiliated Archives liaison;~~

~~(2) Supervisors contact the appropriate office that is the liaison for the affiliate; and,~~

~~(3) The office of liaison may request that NGC review the relevant affiliated archives agreement.~~

1462.8 When does NARA take action to recover alienated records?

Our ability to document the circumstances of removal and establish Federal Government ownership of the materials may affect our assertion of title; each case must be assessed individually before taking any action.

a. NARA always seeks the return of records alienated by loss or theft from NARA's custody (both physical and legal).

b. In other instances, NARA determines on a case-by-case basis whether to seek recovery or allow the records to continue to be maintained by the current holder of the records, if the holder is an institution that can preserve and provide public access to the records consistent with NARA standards. NARA may request a copy of records maintained by the institution in some circumstances. For information about Affiliated Archives agreements, see NARA 1501, Custody of Federal Records of Archival Value. For information on Affiliated Archives applications and their review process, see NARA 1502, Procedures for Processing Proposals for Affiliated Archives.

The following chart provides a basic outline on NARA decision making:

If the records are…	…then
• Federal records accessioned by NARA, including accessioned records located at an affiliated archives • Presidential records (from January 20, 1981 to present) that have been transferred to NARA, excluding records for incumbent Presidents • Donated historical materials accessioned by a Presidential library or the National Archives of the United States • Nixon Presidential materials held by NARA	NARA seeks, without exception, the physical return of such records by appropriate means, including legal action if necessary.
• Federal records currently held by a non-Federal entity that are closely associated with NARA archival holdings	NARA seeks such records if we determine that the records should have come to NARA under an approved records schedule or under Federal law and the records warrant accessioning. NARA may explore establishing the non-Federal entity as an affiliated archives in some situations.
• Presidential or Vice Presidential materials covered by a deed of gift with NARA but currently held by a non-Federal entity	In coordination with the former President or Vice President, as appropriate, NARA seeks such records if we determine that the records should have come to NARA and that the records warrant depositing in a Presidential library.
• Supreme Court or Congressional records that have been on deposit with NARA	In coordination with the Supreme Court or the Congress, NARA may assist with the recovery of such records at the Court's or Congress's request.

1462.9 How does NARA seek the return of records that belong in NARA's custody?

a. If there is evidence that the alienation of NARA holdings was the result of theft or other criminal misconduct then the OIG will work with appropriate Federal and/or state prosecutors to recover the holdings. If prosecution is declined or no criminal conduct is involved, OIG will work as needed with NGC to recover the material.

b. If NGC determines, in consultation with the appropriate office (L or R), and the OIG, as appropriate, that records identified through the procedures in par. 1462.7 should have been, but never were in NARA's physical or legal custody, NGC establishes and presents the case for return of the records to NARA custody to the Archivist for a final decision.

(1) If the Archivist determines that the records belong in NARA's physical or legal custody, NGC works to recover the records from the current custodian, including by:

(aa) Notifying the current custodian of the records of NARA's interest and provides our reasons for seeking return of the records;

(bb) Requesting that the records be safeguarded until NARA determines whether the records should be physically transferred to NARA; and,

(cc) Asking the current custodian how the records came into his or her custody.

(dd) Seeking recovery through donation or other voluntary settlement.

(2) If the current holder of the records does not agree to voluntarily return the records to NARA, NGC may initiate litigation, in coordination with the Department of Justice, and may request assistance from OIG. OIG may open an investigation leading to recovery. If recovery does not occur as a result, OIG works, as needed, with NGC to assist with recovery action.

1462.10 How does NARA decide whether to seek recovery of records that were never in our custody?

The decision to pursue the recovery of Federal records, Presidential and Vice Presidential records, Nixon Presidential historical materials, and donated historical materials, including artifacts, that were never in our custody is made on a case-by-case basis. Because the background research and other resources needed to prepare for a recovery action can be substantial, the alienated record must be both worth the effort and clearly a Federal record that would be accepted in a court of law (particularly if a formal replevin action needs to be taken through the courts). Among the evidence of Government possession that can serve as proof are: distinctive file markings and references in registers, microfilm, or other preservation copies. Accordingly, NARA considers the following criteria in making this decision:

a. The content and the context of the alienated record or records clearly fit into a series of records or into a record group legally owned by the National Archives. (Note: the records could be in an Affiliated Archives, in which case they would not be physically in NARA, but would still be owned by NARA.)

b. The record can easily be identified as Federal in nature. That is, the record has clearly visible file markings or other indicators that it was received and filed by the Federal government; or there are reliable and authentic register entries, microfilm or other copies, or other information that indicate receipt by the Government.

c. Upon examination of applicable records schedules, deposit agreements, or other documentation, we have no reason to believe the record left government custody in accordance with authorized disposition instructions.

d. The record has sufficient special value to justify the replevin effort. L or R archivists must furnish documentation to NGC in support of this value determination based on the guidance in par. 1462.11.

1462.11 How do we determine special value?

a. We use this term in connection with recovery actions when NARA determines that it must take custody of an original record because of qualities in a record that a copy does not adequately convey.

b. Some indicators of special value are:

(1) Association with an important person, place, thing, issue, or historical event;

(2) The informational or evidential content of the record;

(3) The record's format or media, such as unique art, graphics, or other factors that give the record exhibit potential inherent in the original record; and

(4) Appeal to researchers or other special communities of users of NARA holdings such as military and war historians, local historians, historic preservationists, transportation historians, tribal historians, and others.

c. Some records could be associated with an important person, place, event, thing, issue, or historical activity, but not have significant informational or evidential content. Such records may not possess sufficient special value to warrant recovery.

d. A record must have significant special value to justify the extraordinary effort required to initiate replevin action of an item that was never in NARA's custody.

e. In most cases, all four criteria listed in subpar. b should apply to an item to make the recovery effort worthwhile.

1462.12 Does NARA have any examples of how the process of determining special value works?

Yes. The following examples may be helpful:

a. Example One:

(1) A web search revealed the pending sale of a letter from Abraham Lincoln appointing George Harrington to serve temporarily as Secretary of the Treasury in the absence of Salmon P. Chase.

(2) Analysis of images of the document and R holdings indicated that this appointment letter was received and recorded by the Department of State but that it was not filed following registration.

(3) Further, the entire text of the appointment letter had been entered in volume 2 of the Department of State's series of Temporary Presidential Commissions.

(4) R concluded that replevin was not warranted in this case because "the content of the letter is routine and the entire text is in our files in the official record book."

b. Example Two:

(1) A web search uncovered a letter offered for sale from the Secretary of War Jefferson Davis to the Attorney General concerning the relationship of the Articles of War to the cadets of the Military Academy.

(2) Analysis showed that receipt of this letter had been registered by the Attorney General and that R holdings include other letters registered as having been received at the same time and under similar circumstances, as well as the Attorney General's legal opinion responding to the letter.

(3) However, additional evidence indicated that this particular letter had never been in R custody.

(4) Because this document clearly fit into a series of records in R custody, had markings supporting its identity as a Federal record that was not authorized for disposal, involved important officials and concerned an important topic, R recommended that action be taken to recover the item. Recovery was achieved through a donation.

1462.13 How are records created by this directive maintained under the NARA records schedule?

a. NGC - Maintain records under file no. 1101, General Legal files or 1105, Litigation files, as appropriate.

b. OIG - If theft is suspected or reported, maintain records under file no. 1208, Investigative Case files.

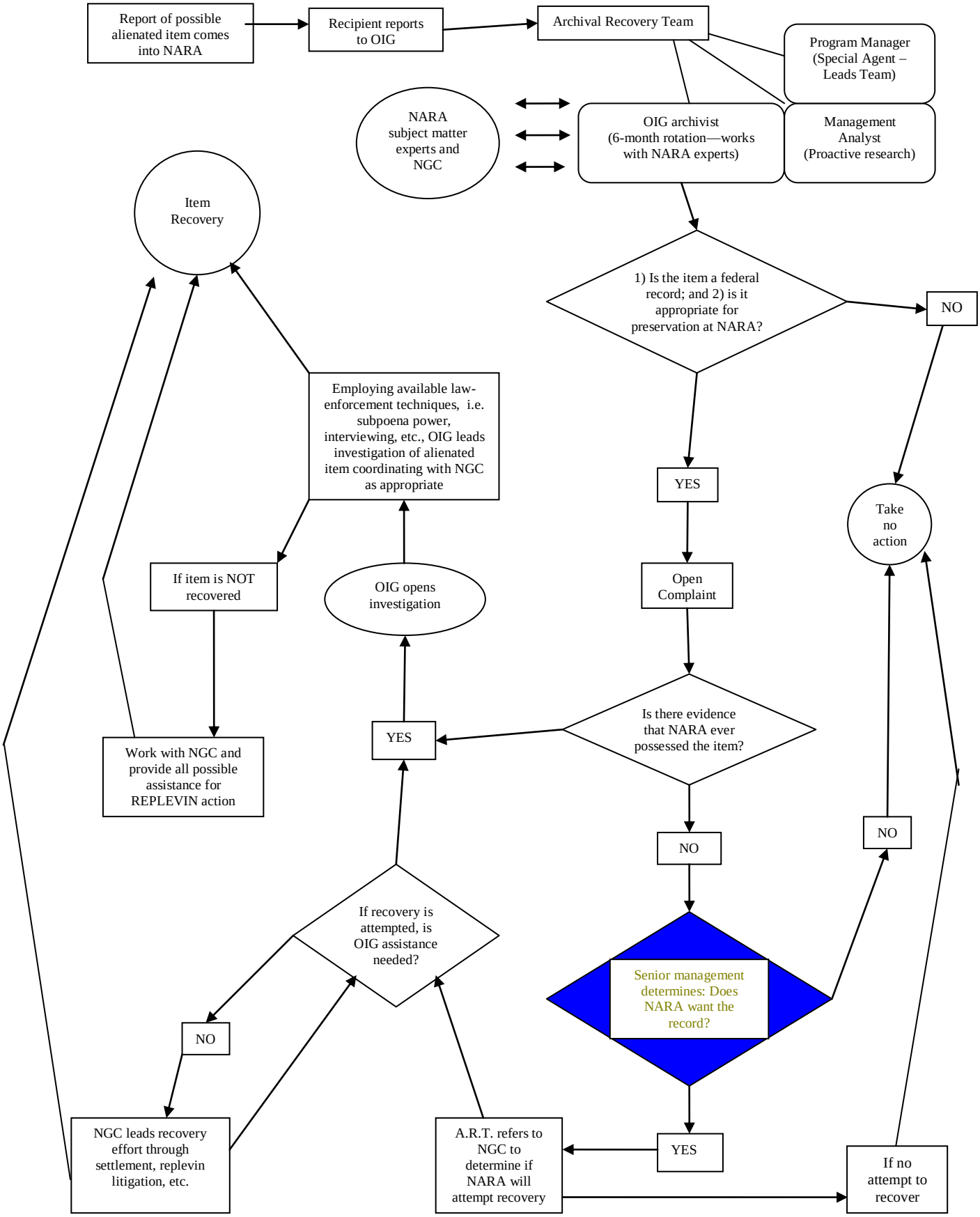
c. If the matter results in an accession, acquisition or proposal to establish an affiliated archives:

(1) Custodial units - If an accession or acquisition results, maintain records L and R units would use file no. 1405 accession dossiers or 1409 acquisition case files (Presidential / Donated materials).

(2) Affiliated archives proposals - Records created by responsible offices and the review panel are currently unscheduled. They may not be destroyed until further notice (when a disposition has been approved by the Archivist of the United States.) Also see NARA 1502, par. 14.

d. All other units - Maintain records under the appropriate program subject file (e.g., 109-2b).

This page intentionally left blank.


Report of possible alienated item comes into NARA
Recipient reports to OIG
Archival Recovery Team
Program Manager (Special Agent – Leads Team)
NARA subject matter experts and NGC
OIG archivist (6-month rotation—works with NARA experts)
Management Analyst (Proactive research)
Item Recovery
1) Is the item a federal record; and 2) is it appropriate for preservation at NARA?
NO
Employing available law-enforcement techniques, i.e. subpoena power, interviewing, etc., OIG leads investigation of alienated item coordinating with NGC as appropriate
YES
Take no action
If item is NOT recovered
OIG opens investigation
Open Complaint
Work with NGC and provide all possible assistance for REPLEVIN action
YES
Is there evidence that NARA ever possessed the item?
NO
NO
If recovery is attempted, is OIG assistance needed?
Senior management determines: Does NARA want the record?
NO
NGC leads recovery effort through settlement, replevin litigation, etc.
A.R.T. refers to NGC to determine if NARA will attempt recovery
YES
If no attempt to recover

National Archives and Records Administration

NARA 1463
March 27, 2003

SUBJECT: Unauthorized Destruction or Removal of Federal Records at Agencies

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a new directive that outlines measures that must be taken to act on actual or alleged instances of records being improperly destroyed by or removed from the custody of Federal agencies.

Why are we issuing this directive? Agency Services (A) has responsibilities for assisting the records management programs in Federal agencies. This directive informs staff of measures that must be taken to inform agencies about allegations of unauthorized disposal of Federal records by destruction or removal. These measures will help ensure the protection of permanent records and temporary records important for citizen rights and Government accountability.

JOHN W. CARLIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1463
March 27, 2003

SUBJECT: Unauthorized Destruction or Removal of Federal Records at Agencies

1463.1 What is the purpose of this directive?
This directive provides measures that must be taken to act on actual or alleged instances of records being improperly destroyed by or removed from the custody of Federal agencies. These measures are to inform agencies about allegations of unauthorized disposal to help ensure the protection of permanent records and temporary records important for citizen rights and Government accountability.

1463.2 What is the authority for this directive?
44 U.S.C. 2905, 44 U.S.C. 3106, and 44 U.S.C. 3311

1463.3 What records are not covered by this directive?
This directive does not address records that have been accessioned into the National Archives of the United States (see NARA 1462, Recovery of Archival Materials) or possible accidental improper implementation of disposition instructions in records centers. This directive also does not address records covered by the Presidential Records Act.

1463.4 Definitions

a. **Agency--**any executive agency that creates Federal records or an establishment in the legislative or judicial branch of the Government (except the Supreme Court, the Senate, the House of Representatives, and the Architect of the Capitol and any activities under the direction of the Architect of the Capitol).

b. **Donation--**an addition to holdings acquired without monetary consideration and becoming the sole property of the recipient, frequently effected by a deed of gift. (Agencies may donate temporary Federal records only with prior NARA approval.)

c. **Personal papers**--the private documents accumulated by or belonging to an individual and subject to his or her disposition.

d. **Unauthorized disposal**--the improper removal of records without NARA approval or the willful or accidental destruction of records without regard to a NARA-approved records schedule.

1463.5 Who is responsible for implementing this directive?

a. Records Management Services (ACNR) works with agencies to resolve allegations and instances of unauthorized destruction or removal. Specific actions are listed in pars. 1463.7 through 1463.10.

b. On a case-by-case basis, and when requested by Agency Services, the General Counsel (NGC) advises the Archivist on measures to take, including whether to request redress by the Attorney General, if necessary.

1463.6 When may records be destroyed, donated, or removed from Federal custody?

a. Records may only be destroyed in accordance with a NARA-approved records schedule. The only exception to this may occur under certain conditions in time of war or when hostile action seems imminent outside the continental United States (see 44 U.S.C. 3311).

b. Agencies may donate temporary records that have been retained for the prescribed retention period to a non-Federal entity only by obtaining NARA approval following the process in 36 CFR 1228.60.

c. Agencies may not loan permanent or unscheduled records to a non-Federal entity without first obtaining NARA approval following the process in 36 CFR 1228.70 through 1228.78.

d. Agencies may not transfer their records to another agency without first obtaining NARA approval following the process in 36 CFR 1228.120 through 1228.136.

e. NARA provides detailed online disposition guidance to agencies in *Disposition of Federal Records*. In addition, *Documenting Your Public Service* gives information about removal of personal papers and copies to avoid the accidental removal of records.

1463.7 How does NARA handle allegations of improper destruction or removal?

a. NARA brings to the attention of agency records officers allegations of actual, impending, or threatened improper removal or destruction of records. NARA always follows up on direct information from an individual. We refer credible allegations of improper action to the agency in accordance with this paragraph and pars. 1463.8 through 1463.10. NARA wants to make sure that agencies are informed about allegations so that they may address them and take action as necessary to avoid a recurrence.

b. If a written allegation is received, immediately hand-carry or fax it to ACNR with copies to NGC, the Communications and Marketing Staff (SC), and the Congressional Affairs Staff (NCON).(. ACNR assigns followup responsibility to the staff member assigned to that agency. If the information is received verbally, prepare a memo for the record describing the information received and handle it as a written allegation.

c. For allegations of impending destruction or removal, the responsible staff member must contact the agency records officer by telephone within two workhours. If the records officer is not immediately available, notify NGC, who contacts the agency's general counsel.

d. For allegations of actual destruction or removal, NARA contacts the agency informally first, then refers the allegation formally to the agency in accordance with this

paragraph and pars. 1463.8 through 1463.10.

e. With allegations of either impending or actual destruction or removal, within five workdays the assigned staff member prepares for AC's signature a letter containing the information in par. 1463.9. After signature, AC sends and faxes the letter to the agency's headquarters records officer with copies to NGC,SC, and NCON..

1463.8 What does NARA do when the allegation comes from within the disposing agency?

a. When an allegation comes from a source within an agency, but an official notification of error has not come from the agency, procedures may be modified to accommodate the particular circumstances. In such cases, ACNR notifies the records officer or other appropriate agency official, following the procedures in par. 1463.7. If the agency source wishes to remain anonymous, NARA honors that request whenever practicable.

b. If an official notification comes from the records officer, AC may determine that notification of another official within an agency, such as the general counsel, is appropriate if the records officer has not already done so. If contact with the agency's general counsel is advisable, AC notifies NGC to discuss the case. If necessary, NGC contacts the agency's general counsel to learn more about the agency's corrective action.

1463.9 What must the letter to the agency contain for cases of actual destruction or removal?

a. Describe the allegation and any facts as NARA understands them.

b. Describe the type of records (for example, planning files, training reports, program briefings, operating program progress reports). Include the name of the records series, dates, and possible subject matter, if possible.

c. Identify the office of origin (program office) and office of custody (office in actual possession of the records at the time of destruction or removal) if available.

d. Identify the disposition authority and disposition instructions for the records, if these can be determined.

e. Indicate the source of the allegation (for example, newspaper article or letter from private citizen). If the allegation appeared in the press or was made by a private citizen in correspondence to NARA, include a copy of the press clipping or letter.

f. Mention any other information that would assist the agency in its investigation, such as date(s) destruction or removal occurred, method of destruction, or circumstances under which records were destroyed or removed.

g. Ask the agency records officer (or official to whom the letter is addressed) to

investigate the matter, citing NARA's statutory authority in 44 U.S.C. 2905.

h. Ask the agency to provide NARA with a report that contains the information required by 36 CFR 1228.104. Include a copy of the regulation with the letter. Require the agency to respond within 30 calendar days of the date of NARA's letter with the information needed to resolve the allegation or steps the agency is taking to investigate the matter and avert further unauthorized disposals or removals.

i. If a communication from a private citizen triggered the unauthorized disposal or removal inquiry, send that person a copy of NARA's letter to the agency with a cover letter signed by AC explaining NARA's action.

1463.10 What must the letter to the agency contain in cases of alleged impending destruction or removal?

As a followup to subpars. 1463.7c and d and in conjunction with subpar. 1463.7e, include in the letter to the agency the same information cited in par. 1463.9, where applicable.

1463.11 How does NARA monitor the agency's response?

a. ACNR maintains a log of all actual or alleged cases and issues quarterly reports on the status of each case to AC, A and NGC.

b. A copy of the letter to the agency is placed in an ACNR tickler file. If the agency does not respond after 30 calendar days, the ACNR work group leader ensures that the responsible ACNR work group staff member contacts the agency. If necessary, the responsible ACNR work group staff member drafts a followup letter to the agency for AC signature.

c. When ACNR receives the agency's written response, the responsible ACNR work group staff member analyzes it to determine whether it satisfactorily addresses the allegation. Within five business days of receipt of the agency's response, the responsible work group staff member prepares a letter for AC signature informing the agency that the matter is closed or that additional action or information is required. If the agency is conducting an investigation, NARA keeps the case open until the agency reports a resolution.

d. If a private citizen brought the allegation to NARA's attention, NARA provides that person with copies of the agency response and NARA's followup correspondence.

1463.12 What happens if the agency is unresponsive?

a. If the agency is unresponsive or does not demonstrate appropriate corrective action, ACNR staff may pursue the case through the chain of command to A. If A agrees that the agency was not responsive, the Executive discusses possible further action with NGC. A also notifies the Deputy Archivist the Executive for Strategy and Communications and NCON.

b. If the case warrants further action, NGC writes to the general counsel and the inspector general of the pertinent agency outlining the status of the case and requesting additional information or action within 30 calendar days.

c. If attempts to resolve the case through the agency's general counsel are unsuccessful, NGC and the Archivist determine the appropriate action. This may include sending a letter from the Archivist to the head of the agency or contacting the Department of Justice.

National Archives and Records Administration

Transmittal Memo

DATE: June 1, 2013

TO: Executives, Staff Directors, , NHPRC, and OIG

SUBJECT: NARA 1464, Destruction of Federal Records in the Custody of NARA Records Centers

Purpose: This transmits a revised policy directive, NARA 1464, Destruction of Federal Records in the Custody of NARA Records Centers.

Background/significant changes: Supplement revised to reflect current procedures. Federal Record Center staff should continue to use local procedures until further notice.

Available forms: SF 115, Request for Records Disposition Authority.

Canceled policy: This directive cancels NARA 1464, Destruction of Federal Records in the Custody of NARA Records Centers, dated December 21, 2010.

Canceled forms: None.

Effective date: This directive is effective date of signature.

Contact information: Questions regarding this directive should be addressed to Russell F. Loiselle in Operations Branch (AFO), on (301) 837-3527 or at Russell.Loiselle@nara.gov.

DAVID S. FERRIERO
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1464
June 1, 2013

SUBJECT: NARA 1464, Destruction of Federal Records in the Custody of NARA Records Centers

1464.1 What is the purpose of this directive?

This directive establishes NARA's policy for disposing of Federal records in the custody of NARA records centers.

1464.2 What are the authorities for this directive?

a. 44 U.S.C. Chapter 33

b. 36 CFR part 1226, Implementing Disposition

c. 36 CFR part 1229, Emergency Authorization to Destroy Records

d. 36 CFR part 1230, Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records

e. 36 CFR part 1233, Transfer, Use and Disposition of Records in a NARA Federal Records Center

1464.3 What records are not covered by this directive?

This directive does not address records that have been accessioned into the National Archives and Records Administration of the United States (see NARA 1462, Replevin of Archival Materials) or records actually or allegedly being improperly destroyed by or removed from the custody of Federal agencies (see NARA 1463, Unauthorized Destruction or Removal of Federal Records at Agencies). This directive also does not address records covered by the Presidential Records Act.

1464.4 To whom does this directive apply?

This directive applies to all NARA federal records centers.

1464.5 Definitions of terms used in this directive

a. **Erroneous disposal** - the accidental destruction of records in a records center without regard to a NARA-approved records schedule and without the agency's written concurrence.

b. **Records disposition schedule** - a document, having legally binding authority when approved by NARA that provides mandatory instructions (i.e., disposition authority) for what to do with records no longer needed for current business. Examples include an approved Standard Form 115, Request for Records Disposition Authority, a published agency manual, or instruction based on a NARA-approved SF 115.

1464.6 Who is responsible for implementing this directive?

The Federal Records Center Program (AF) directors are responsible for all activities associated with the disposal of records. They ensure that records are properly disposed of in accordance with appropriate records disposition schedules and receipt of written concurrence from the agency.

1464.7 What records may be destroyed?

Records generally may be destroyed only if they have reached the end of their retention period, as stipulated in a NARA-approved records schedule, and if the records center has received written agency concurrence for their destruction. See supplement for general information detailed procedures. (Some records may be eligible for donation and removal from Federal custody, in lieu of physical destruction. See NARA 1463, Unauthorized Destruction or Removal of Federal Records at Agencies for additional information.)

1464.8 Are there times when agencies and NARA can properly dispose of records prior to the date indicated on the records disposition schedule?

Yes, such as when records are a continuing menace to health or life, or to property (such as radiation-contaminated records and those contaminated by various biological and chemical hazards) or during a state of war or threatened war.

1464.9 Must erroneous disposals of records be reported?

Yes, erroneous disposals of records are reported by individuals to the AF Director, who notifies the Executive for Agency Services (A), who in turn notifies the Archivist of the United States (N), See supplement for information to be included in the report, timing of notification, and other offices which need to be notified.

1464.10 Can employees anonymously report an erroneous disposal of records?

Yes. Employees may anonymously report erroneous disposal of records directly to the Office of Inspector General (OIG) through the "OIG Hotline" (www.archives.gov/oig/hotline.html).

1464.11 How are records created by this directive maintained under the NARA Records Schedule?

Maintain records created and received under this directive in accordance with File No. 1343-3 in the NARA Record Schedule (N1-64-07-5).

National Archives and Records Administration

Transmittal Memo

DATE: January 29, 2015

TO: Executives, Staff Directors, NHPRC, and OIG

SUBJECT: NARA 1464-S1, Disposal Procedures for Temporary Records

Purpose: This transmits a revised NARA 1464-S1, Disposal Procedures for Temporary Records, a supplement to NARA 1464, Destruction of Federal Records in the Custody of NARA Records Centers.

Background/significant changes: Procedures previously included as a supplement have been revised to reflect current standard operating procedures.

Available forms: None.

Canceled policy: This directive cancels NARA 1464-S1, Disposal Procedures for Temporary Records, dated February 10, 2014.

Canceled forms: None.

Effective date: This directive is effective date of signature.

Contact information: Questions regarding this directive should be addressed to Russell F. Loiselle in Operations Branch (AFO), on (301) 837-3527 or at Russell.Loiselle@nara.gov.

JAY TRAINER
Executive for Agency Services

Attachment

National Archives and Records Administration

General Information

Written concurrence is acceptable in many forms
NARA's Counsels Office has made the determination that a "wet" signature is not mandatory for proof of agency concurrence when a reasonable assumption of trustworthiness can be implied *[Hannah Bergman 09/17/2013 Decision Email]*.

Acceptable forms of written concurrence may include:

- A "wet" signature on an original NA-13001.
- A single signed cover memo which lists all transfers approved for disposal.
- An email or fax from the official POC stating specifically which transfer(s) approved for disposal.
- A PDF of a signed (or digitally signed) NA13001 or a single cover memo (and attachments) if it comes from a reliable POC.

Written concurrence received after a Report 22 has been generated, but before the beginning of the disposal cycle
Request a new Report 22 or write all the pertinent transfer data on the appropriate page.

Written concurrence received after the initial 90-day period
Do not change the disposal date to the next cycle. These transfers will automatically appear on the next cycle's Report 22.

All disposals must be witnessed either by a Government employee or contractor employee
All disposals must be handled as either a Government- or contractor-witnessed disposal. All recycling contracts must include the provision for the issuance of a certificate of destruction for all records after the records have been destroyed.

At-Risk Transfers Report
All FRCs should perform the "At Risk" review at least once per week, and more frequently when needed (for example, when an FRCP Freeze Advisory is issued). During disposal cycles, this review is conducted daily until disposal is final.

When destroying Federal tax information, the following guidelines must be observed

Burning precautions: The material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle must be separated to ensure that all pages are consumed.

Shredding precautions: To make reconstruction more difficult, insert the paper so that lines of print are perpendicular to the cutting line and not maintain small amounts of shredded paper. If disposal is a one-step shredding process, shred the paper to 5/16-inch wide or smaller strips; shred microfilm to 1/35-inch by 3/8-inch strips. If shredding is part of an overall two-step process of destruction of IRS data, strips can be set at the industry standard (currently ½"). However, when deviating from the IRS 5/16" requirement, IRS data as long as it is in this condition (i.e., strips larger than 5/16"), must be safeguarded until it reaches the stage where it is rendered unreadable.

Pulping precaution: Accomplish pulping so that all material is reduced to particles one inch or smaller.

Reporting an Unauthorized Disposal at a NARA FRC

Per NARA 1464.9, all unauthorized disposals of records must be reported.

When an unauthorized disposal is discovered, FRC staff should notify the Director of the affected FRC(s) within one (1) working day via telephone.

The FRC Director(s) should report the incident in writing within three (3) working days to the Director, Federal Records Centers Program.

The incident report must include the following information:

a. A complete description of the records with volume and dates, if known;

b. The office of origin;

c. A statement of the exact circumstances surrounding the destruction of the records;

d. A statement of the safeguards established to prevent further loss of documentation;

e. When appropriate, details of the actions taken to salvage, retrieve, or reconstruct the record; and

f. A detailed draft letter to the agency that controls access to the records that will be finalized for signature by the Director of the Federal Records Centers Program.

The Director of the Federal Records Centers Program notifies the Executive for Agency Services and the Chief Records Officer, and copies the Chief Operating Officer, the Deputy Archivist, and the Archivist.

The Director of the Federal Records Centers Program finalizes and signs the draft letter submitted by the FRC Director and sends it to the agency customer. The customer agency may also be notified by other means (telephone, email, etc.).

Review of Records Eligible for Disposal Report (Report 23)

No.	Activity	Detailed Description	Responsible Party
1	**Compare transfers listed on Records Eligible for Disposal Report (Report 23) against SF 135s**	**NOTE: This is the first review, conducted by the Transfer and Disposition Specialist or a Subject Matter Expert.**	Transfer and Disposition Specialist (TDS) or Subject Matter Expert (SME)
1.1	For each transfer listed on the Report 23, locate the original SF 135 and attach in ARCIS.	Check the SF 135 files/library, the purged SFs 135 files, and/or the first box of the transfer for the SF 135. As a last resort, if you cannot locate the original SF 135, contact the agency for a copy. If you locate the original SF 135 (or obtain a copy), scan and attach it to the transfer in ARCIS and then proceed to 1.2. If you cannot locate the original SF 135 (or obtain a copy), proceed to 1.1.1.	TDS
1.1.1	If necessary, print a replacement SF 135.	From the ARCIS records transfers tab, print a replacement SF 135 for the Transfer and then scan and attach it to the transfer in ARCIS. **NOTE:** If you have to print an ARCIS SF 135, you will need to check the SF 135 against the **box contents** rather than against the Report 23. In other words, in steps 1.2.1 through 1.2.9, **you must physically check the boxes** to validate that each of the critical data fields on the ARCIS SF 135 is correct.	TDS
1.2	For each transfer listed on the Report 23, check critical data fields to ensure that the information matches that on the SF 135.	Note: The SF 135 review is conducted using the scanned SF 135 in ARCIS.	TDS/SME

No.	Activity	Detailed Description	Responsible Party
1.2.1	Series Description	If the Series Description matches (except for minor typos), proceed to 1.2.2. If the Series Description does not match and the discrepancy is not merely minor typos, check the box contents to determine which series description is correct. Mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use ARCIS Transaction Administration to make changes to the ARCIS transfer record. Annotate the Report 23 to indicate what changes were made and why.	TDS/SME
1.2.2	Disposition Authority	If the Disposition Authority matches, check the Records Control Schedule to ensure that this is the correct authority for the records series. If the Disposition Authority matches AND if it is correct, proceed to 1.2.3. If the Disposition Authority does not match OR if it is not correct, check to see whether a data change was made that affected the Disposal Authority for the transfer. If so, mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use the ARCIS Transaction Administration tab to make changes to the transfer record in ARCIS. Annotate the Report 23 to indicate what changes were made and why. Print or photocopy any materials that document the changes, such as memos or schedule crosswalks.	TDS/SME

No.	Activity	Detailed Description	Responsible Party
		If you cannot resolve the issue, line out the transfer on the Report 23. In ARCIS, set the transfer's status back to "Shelved." Stop working on this transfer and begin checking the next transfer on the Report 23.	
1.2.3	Beginning Date	This needs to be reviewed only if the Disposition Date is based on the Beginning Date. If not, proceed to 1.2.4. If the Beginning Date matches, proceed to 1.2.4. If the Beginning Date does not match, call the agency to ask which date is correct. If the correct date cannot be provided by the agency, physically check the records to determine the correct date. Mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use the ARCIS Transaction Administration tab to make changes to the transfer record in ARCIS. If you change the beginning date in ARCIS, be sure to recalculate the Disposition Date. Annotate the Report 23 to indicate what changes were made and why.	TDS/SME
1.2.4	Ending Date	If the Ending Date matches, proceed to 1.2.5. If the Ending Date does not match, call the agency to ask which date is correct. If the correct date cannot be provided by the agency, physically check the records to determine the correct date. Mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use the Transaction Administration tab make changes to the transfer record in ARCIS. If you make any changes to the date in ARCIS, and if the Disposition Date is based on the Ending Date, recalculate the Disposition Date. Annotate the Report 23 to indicate what changes were made and why.	TDS/SME

No.	Activity	Detailed Description	Responsible Party
1.2.5	Disposition Date	If the Disposition Date matches, use the retention period indicated on the Report 23 to check whether the date calculation is correct. If the Disposition Date matches AND if the date calculation is correct, proceed to 1.2.6. If the Disposition Date does not match OR if the date calculation is not correct, perform the following checks: • Was there a prior Declined or Cancelled 13001 that altered the date? • Was there a retention period change made to that particular authority? • Was there a beginning or ending date change that could have affected the disposition date? Mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use the Transaction Administration tab make changes to the transfer record in ARCIS. Annotate the Report 23 to indicate what changes were made and why. If you cannot resolve the issue, line out the transfer on the Report 23. In ARCIS, set the transfer's status back to "Shelved". Stop working on this transfer and begin checking the next transfer on the Report 23.	TDS/SME
1.2.6	Volume	If the Volume matches, proceed to 1.2.7. If the Volume does not match, perform the following checks: • Determine whether the transfer was created in NARS-5 and sub-	TDS/SME

No.	Activity	Detailed Description	Responsible Party
		transfers with Alpha characters were used. If so, these need to be added to obtain the total volume. • Determine whether any assets were permanently withdrawn (PW). Check ARCIS and/or check to see whether a legacy PW charge-out is attached to the SF 135. • Physically verify the volume on the shelves. If containers are missing, determine the reason. • Determine whether the discrepancy is due to the use of non-standard containers. Once you have determined the correct volume, mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use the Transaction Administration tab to make changes to the transfer record in ARCIS. Annotate the Report 23 to indicate what changes were made and why.	
1.2.7	Beginning and Ending Box Numbers (Container Numbers)	This needs to be reviewed only if the transfer is a legacy (pre-ARCIS) transfer. If not, proceed to 1.2.8. If the Container Numbers match, proceed to 1.2.8. If the Container Numbers do not match, use the Transaction Administration tab make any necessary changes to the transfer record in ARCIS.	TDS/SME
1.2.8	Disposition Code	If the Disposition Code matches AND if it is either “Temporary” or “Temporary Contingent,” proceed to 1.2.9. If the Disposition Code does not match OR if it is not “Temporary” or “Temporary Contingent,” check the Records Control Schedule to	TDS/SME

No.	Activity	Detailed Description	Responsible Party
		determine the correct code. Mark any necessary pen and ink changes on the SF 135 (note that the changes were made by FRC staff and the date) and/or use the Transaction Administration tab make changes to the transfer record in ARCIS. Annotate the Report 23 to indicate what changes were made and why. If the correct code is anything other than "Temporary" or "Temporary Contingent," line out the transfer on the Report 23. In ARCIS, set the transfer's status back to "Shelved." Stop working on this transfer and begin checking the next transfer on the Report 23.	
1.2.9	Classification Level	If the Classification Level matches, you're done checking data fields on this transfer. Go back to 1.2.1 and begin checking the next transfer. If you've checked all the transfers on the Report 23, proceed to 2. If the Classification Level does not match, use the Transaction Administration tab make changes to the transfer record in ARCIS. If the correct classification is higher than what was originally in ARCIS, follow the Security Incident Reporting process. Then go back to 1.2.1 and begin checking the data fields on the next transfer—or, if you've checked all the transfers on the Report 23, proceed to 2.	TDS/SME
2	**Review and Verify Freeze Codes.**		TDS/SME
2.1	Check ARCIS for transfers that are "At Risk."	Check to see whether any of the transfers on the Report 23 have been tagged in ARCIS as "At Risk." If so, determine why the transfer has been tagged as "At Risk." If you are able to resolve the issue, make the necessary changes in	TDS/SME

No.	Activity	Detailed Description	Responsible Party
		ARCIS. Put a checkmark in the "Resolved" box and, in the Comments field, provide an explanation of how the issue was resolved. If you cannot resolve the issue, line out the transfer on the Report 23. In ARCIS, set the transfer's status back to "Shelved."	
2.2	Check SF 135s and freeze files for freezes.	For each transfer on the Report 23, check the SF 135 to see whether the retiring office requested a freeze. Then check the disposition authority against the Master Freeze Log (\\A2U2SHARED\A2U2SHARED\SHARED\NC\FEDERAL RECORDS CENTERS PROGRAM\Transfer & Disposition\Freeze Information\Master Freeze Log) and locally maintained "freeze files" to see whether a freeze was requested. If all transfers are verified to be free of freeze codes, proceed to 3. If a freeze code should have been applied or is pending application, line out the transfer on the Report 23. In ARCIS, set the transfer's status back to "Shelved." Send a "high priority" email to the National T&D Operation (Freeze Coordinator) requesting that the appropriate freeze code be applied. NOTE: Freezes are no longer applied locally. All are processed by the Freeze Coordinator.	TDS/SME
3	**Prepare for TDC/DD review.**	If any corrections were made/annotated to the original SF 135, rescan and attach the latest version to the transfer in ARCIS.	TDS
3.1	Create Disposition Notifications.	After all items above have been completed, query ARCIS for transfers that are still eligible for disposal. Check each transfer against the Report	TDS

No.	Activity	Detailed Description	Responsible Party
		23 to verify that it is not lined out, then put a checkmark in the "Ready for Disposal" field. Create Disposition Notifications for the eligible transfers. Under the Disposition Notifications tab, run a "Notification Initiated" query. Export the query report to include in the package for the next reviewer. Before passing the query report on to the next reviewer, verify that the Charge Account, Retiring Office, and Disposal Approver are correct for each transfer.	
3.2	Approve for review.	Sign and date the annotated Report 23 to verify that all actions have been completed. Give the TDC or DD: • the annotated Report 23 • the "Notification Initiated" query report	TDS

4	**Compare transfers listed on Records Eligible for Disposal Report (Report 23) against SF 135s attached in ARCIS.**	**NOTE: This is the second review, conducted by the Transfer and Disposition Chief, the Deputy Director, or an approved Subject Matter Expert; if the initial review is by a Subject Matter Expert the second review may be performed by the Transfer and Disposition Specialist. There is no longer a 100% check requirement.** **ALL transfers lined out or noted as a potential error with the symbol "!" on the Report 23 must be reviewed. This includes checking ARCIS to be sure that lined-out transfers were handled correctly.** **For each lined out or potential-error transfer, check the following data fields.**	Transfer and Disposition Chief (TDC) or Deputy Director (DD) or **Subject Matter Expert (SME) or Transfer and Disposition Specialist (TDS)**
4.1	Series Description	If the Series Description matches, proceed to 4.2.	TDC, DD, SME or TDS

No.	Activity	Detailed Description	Responsible Party
		If the TDS made any changes, check them. If they are accurate, proceed to 4.2. If the TDS overlooked a mismatch, or if changes were not made correctly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	
4.2	Disposition Authority	If the Disposition Authority matches, proceed to 4.3. If the TDS made any changes, check them. If they are accurate, proceed to 4.3. If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
4.3	Beginning Date	This needs to be reviewed only if the Disposition Date is based on the Beginning Date. If not, proceed to 4.4. If the Beginning Date matches, proceed to 4.4. If the TDS made any changes, check them. If they are accurate, proceed to 4.4. If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
4.4	Ending Date	If the Ending Date matches, proceed to 4.5.	TDC, DD, SME or TDS

No.	Activity	Detailed Description	Responsible Party
		If the TDS made any changes, check them. If they are accurate, proceed to 4.5. If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	
4.5	Disposition Date	If the Disposition Date matches, use the retention period indicated on the Report 23 to check whether the date calculation is correct. If the Disposition Date matches AND the date calculation is correct, proceed to 4.6. If the TDS made any changes, check them. If they are accurate, proceed to 4.6. If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
4.6	Volume	If the Volume matches, proceed to 4.7. As you check the Volume, keep in mind that if the transfer was created in NARS-5, there could be sub-transfers with Alpha characters that need to be added to obtain a total volume. Also keep in mind that billable volume in ARCIS will not match the container count if the transfer is in non-standard containers. If the TDS made any changes, check them. If they are accurate, proceed to 4.7.	TDC, DD, SME or TDS

No.	Activity	Detailed Description	Responsible Party
		If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	
4.7	Beginning and Ending Box Numbers (Container Numbers)	This needs to be reviewed only if the transfer is a legacy (pre-ARCIS) transfer. If not, proceed to 4.8. If the Container Numbers match, proceed to 4.8. If the TDS made any changes, check them. If they are accurate, proceed to 4.8. If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
4.8	Disposition Code	If the Disposition Code matches AND is either "Temporary" or "Temporary Contingent, proceed to 4.9. If the TDS made any changes, check them. If they are accurate, proceed to 4.9. If the TDS overlooked a mismatch, if changes were made incorrectly, or if the Disposition Code is not "Temporary" or "Temporary Contingent," mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
4.9	Classification Level	If the Classification level matches, you're done checking data fields on this transfer. Go back to 4.1 and begin checking the next transfer. If you've checked all the transfers on the Report 23, proceed to 5.	TDC, DD, SME or TDS

No.	Activity	Detailed Description	Responsible Party
		If the TDS made any changes, check them. If they are accurate, begin checking the data fields on next transfer—or, if you've checked all the transfers on the Report 23, proceed to 5. If the TDS overlooked a mismatch, or if changes were made incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet. Then begin checking the data fields on the next transfer—or, if you've checked all the transfers on the Report 23, proceed to 5.	
5	**Review and Verify Freeze Codes.**		TDC, DD, SME or TDS
5.1	Check ARCIS for transfers that are "At Risk."	Check to see whether any of the transfers not lined out on the Report 23 have been tagged in ARCIS as "At Risk." If so, mark the problem on the Report 23 so that the TDS can follow up. There is no need to document a quality review error, since the transfer may have been tagged after the TDS review.	TDC, DD, SME or TDS
5.1.1	Check SF 135s and freeze files for freezes.	For each transfer on the Report 23, check the SF 135 to see whether the retiring office requested a freeze. Then check the disposition authority against the Master Freeze Log (\\A2U2SHARED\A2U2SHARED\SHARED\NC\FEDERAL RECORDS CENTERS PROGRAM\Transfer & Disposition\Freeze Information\Master Freeze Log) and locally maintained "freeze files" to see whether a freeze was requested.	TDC, DD, SME or TDS

No.	Activity	Detailed Description	Responsible Party
		If all transfers are verified to be free of freeze codes, proceed to 6. If the TDS made any changes, check them. If they are accurate, proceed to 6. If the TDS overlooked a freeze code discrepancy that should have been caught, or if the TDS made changes incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet. If a freeze code discrepancy occurred after the TDS review, simply mark it on the Report 23 so that the TDS can follow up. There is no need to document a quality review error.	
6	**Review the "Notification Initialized" query report.**	Verify that all eligible transfers listed on the Report 23 are also listed on the "Notification Initialized" query report. For each transfer, verify that the Charge Account, Retiring Office, and Disposal Approver listed on the query report are correct. If everything is correct, proceed to 7. If not, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
7	**Check ARCIS for transfers that are "At Risk."**	Check one more time to see whether any of the transfers on the Report 23 have been tagged in ARCIS as "At Risk." If not, proceed to 8. If so, mark the problem on the Report 23 so that the TDS can follow up.	TDC, DD, SME or TDS

No.	Activity	Detailed Description	Responsible Party
8	**Check items removed from the Report 23.**	Were any transfers lined out on the Report 23? If not, proceed to 9. If so, check to see whether all necessary data and status changes were made correctly in ARCIS. If changes were not made correctly, mark the problem on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	TDC, DD, SME or TDS
9	**Prepare for next phase (either corrections or Director review).**	Sign and date the Report 23 to verify that you have completed all steps of your review. Did you mark any problems on the Report 23? If so, return the Report 23 and the other materials to the TDS so that the TDS can make corrections. If no corrections are necessary, give the Report 23, the SF 135s, and the "Notification Initiated" query report to the Director for review.	TDC, DD, SME or TDS
10	**Make and review corrections.**	**NOTE: This step is necessary only if the second-level reviewer marked problems on the Report 23.** TDS: Correct all of the problems that were marked on the Report 23, then return the Report 23 and the other materials to the TDC or DD. TDC or DD: Review the corrections. If any problems remain, mark them on the Report 23 and return the materials to the TDS for additional work. Make note of the quality review error on the appropriate QR accountability sheet. If all problems have been resolved, give the marked-up Report 23 and the "Notification Initiated" query report to the Director for review.	TDS and TDC/DD/SME

No.	Activity	Detailed Description	Responsible Party
		If corrections to the SF 135 were made, rescan and attach the latest version of the SF 135 to the transfer in ARCIS.	
11	**Compare transfers listed on Records Eligible for Disposal Report (Report 23) against SF 135s attached in ARCIS.**	**NOTE: This is the third review, conducted by the Director. It is a sample check. The percentage to be reviewed is at Director's discretion.** **For each of the transfers selected for review, check the following data fields.**	Director (D)
11.1	Series Description	If the Series Description matches, proceed to 11.2. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.2. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D
11.2	Disposition Authority	If the Disposition Authority matches, proceed to 11.3. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.3. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D
11.3	Beginning Date	This needs to be reviewed only if the Disposition Date is based on the Beginning Date. If not, proceed to 11.4.	D

No.	Activity	Detailed Description	Responsible Party
		If the Beginning Date matches, proceed to 11.4. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.4. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	
11.4	Ending Date	If the Ending Date matches, proceed to 11.5. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.5. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D
11.5	Disposition Date	If the Disposition Date matches, use the retention period indicated on the Report 23 to check whether the date calculation is correct. If the Disposition Date matches AND the date calculation is correct, proceed to 11.6. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.6. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D

No.	Activity	Detailed Description	Responsible Party
11.6	Volume	If the Volume matches, proceed to 11.7. As you check the Volume, keep in mind that if the transfer was created in NARS-5, there could be sub-transfers with Alpha characters that need to be added to obtain a total volume. Also keep in mind that billable volume in ARCIS will not match the container count if the transfer is in non-standard containers. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.7. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D
11.7	Beginning and Ending Box Numbers (Container Numbers)	This needs to be reviewed only if the transfer is a legacy (pre-ARCIS) transfer. If not, proceed to 11.8. If the Container Numbers match, proceed to 11.8. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.8. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D
11.8	Disposition Code	If the Disposition Code matches AND is either “Temporary” or “Temporary Contingent,” proceed to 11.9.	D

No.	Activity	Detailed Description	Responsible Party
		If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, proceed to 11.9. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	
11.9	Classification Level	If the Classification Level matches, you're done checking data fields on this transfer. Go back to 11.1 and begin checking the next transfer. If you've checked all the transfers on the Report 23, proceed to 12. If the previous reviewers made any changes or marked any problems, check them. If the changes are accurate and the problems are resolved, begin checking the data fields on the next transfer—or, if you've checked all the transfers on the Report 23, proceed to 12. If problems remain, mark them on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet. Then begin checking the data fields on the next transfer—or, if you've checked all the transfers on the Report 23, proceed to 12.	D
12	**Review and Verify Freeze Codes.**		D
12.1.1	Check SF 135s and freeze files for freezes.	For each transfer on the Report 23, check the SF 135 to see whether the retiring office requested a freeze. Then check the disposition authority against the Master Freeze Log (\\A2U2SHARED\A2U2SHARED\SHARED\NC\FEDERAL RECORDS CENTERS PROGRAM\Transfer & Disposition\Freeze	D

No.	Activity	Detailed Description	Responsible Party
		Information\Master Freeze Log) and locally maintained "freeze files" to see whether a freeze was requested. If all transfers are verified to be free of freeze codes, proceed to 13. If the previous reviewers made any changes, check them. If they are accurate, proceed to 13. If the previous reviewers overlooked a freeze code discrepancy that should have been caught, or if the TDS made changes incorrectly, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet. If a freeze code discrepancy occurred after the previous reviews were completed, simply mark it on the Report 23 so that the TDS can follow up. There is no need to document a quality review error.	
13	**Review the "Notification Initiated" query report.**	Verify that all eligible transfers listed on the Report 23 are also listed on the "Notification Initiated" query report. For each transfer, verify that the Charge Account, Retiring Office, and Disposal Approver listed on the query report are correct. If everything is correct, proceed to 14. If not, mark the discrepancy on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	D
14	**Check items removed from the Report 23.**	Were any transfers lined out on the Report 23? If not, proceed to 15.	D

No.	Activity	Detailed Description	Responsible Party
		If so, check to see whether all necessary data and status changes were made correctly in ARCIS. If changes were not made correctly, mark the problem on the Report 23. Make note of the quality review error on the appropriate QR accountability sheet.	
15	**Check for problems that need correction.**	Did you mark any problems on the Report 23? If so, return the Report 23 and the other materials to the TDC or DD. If no corrections are necessary, proceed to 17. .	D
16	**Make and review corrections.**	**NOTE: This step is necessary only if the Director marked problems on the Report 23.** TDC or DD: Give the Report 23 and the other materials to the TDS so that the TDS can make corrections. TDS: Correct all of the problems that were marked on the Report 23, then return the Report 23 and the other materials to the TDC or DD. TDC or DD: Review the corrections. If any problems remain, mark them on the Report 23 and return the materials to the TDS for additional work. Make note of the quality review error on the appropriate QR accountability sheet. If all problems have been resolved, give the marked-up Report 23, the SF 135s, and the "Notification Initiated" query report back to the Director for review. D: Review the corrections. If any problems remain, mark them on the Report 23 and return the materials to the TDC or DD. Make note of the quality review error on the appropriate QR accountability sheet. If all problems have been resolved, proceed to 17.	TDS, TDC/DD, and D

No.	Activity	Detailed Description	Responsible Party
		If corrections to the SF 135 were made, rescan and attach the latest version of the SF 135 to the transfer in ARCIS.	
17	**Check ARCIS for transfers that are "At Risk"**	As your last step before signing and dating the Report 23 and turning it over for processing, check to see whether any of the transfers on the Report 23 have been tagged in ARCIS as "At Risk." If so, mark the problem on the Report 23 and return it to the TDS for appropriate action. If not, proceed to 18.	D
18	**Return for processing**	Sign and date the Report 23 to verify that you have completed all steps of your review. Return the Report 23 and the other materials to the TDC or DD for processing.	D

Review of Records Disposal Retrieval Report (Report 22)

No.	Activity	Detailed Description	Responsible Party
1	**Compare transfers listed on Records Disposal Retrieval Report (Report 22) against NA 13001s.**	**NOTE: This is the first review, conducted by the Transfer and Disposition Specialist.** For each transfer listed on the Report 22, verify that there is an NA 13001 (or its equivalent). If there is no NA 13001 (or its equivalent), flag the transfer for investigation and resolution. For each matched NA 13001, ensure that: • The "approved" block is checked • The form has been signed and dated by the authorized disposal approver If the "approved" block is not checked or the form has been signed by someone other than the authorized disposal approver, investigate and make changes and/or corrections as needed.	Transfer and Disposition Specialist (TDS)
2	**Check ARCIS for transfers that are "At Risk."**	Check to see whether any of the transfers on the Report 22 have been tagged in ARCIS as "At Risk."	TDS

No.	Activity	Detailed Description	Responsible Party
	Note: This step should be repeated daily until disposal occurs.	If so, determine why the transfer has been tagged as "At Risk." If you are able to resolve the issue, make the necessary changes in ARCIS. Put a checkmark in the "Resolved" box and, in the Comments field, provide an explanation of how the issue was resolved. If you cannot resolve the issue, line out the transfer on the Report 22. In ARCIS, set the transfer's status back to "Shelved."	
3	**Check for pending or potential freezes.**	Check freeze advisories and agency communications for pending or potential freezes. If a freeze is pending or has been requested by an agency: • Line out the transfer on the Report 22. • Cancel disposal by setting the status in ARCIS to "Disposition Canceled." • Advise Freeze Coordinator that freeze needs to be applied.	TDS
4	**Prepare for TDC/DD review**	Sign and date the Report 22 to verify that you have completed all steps of your review.	TDS

No.	Activity	Detailed Description	Responsible Party
		Give the TDC or DD the following: • Report 22 (signed and dated) • NA 13001s and any supporting documents (such as freeze advisories)	
5	**Compare transfers listed on Records Disposal Retrieval Report (Report 22) against NA 13001s.**	**NOTE: This is the second review, conducted by the Transfer and Disposition Chief or the Deputy Director. It is a 100% check.** **ALL transfers—including transfers lined out on the Report 22—must be reviewed.** For each transfer listed on the Report 22, verify that there is an NA 13001 (or its equivalent). If there is no NA 13001 (or its equivalent), mark the discrepancy on the Report 22. For each matched NA 13001 ensure that: • The "approved" block is checked • The form has been signed and dated by the authorized disposal approver	T&D Chief (TDC) or Deputy Director (DD)

No.	Activity	Detailed Description	Responsible Party
		If the "approved" block is not checked or the form has been signed by someone other than the authorized disposal, mark the discrepancy on the Report 22. Make note of the quality review error on the appropriate QR accountability sheet.	
6	**Check ARCIS for transfers that are "At Risk."** **THIS IS A CRITICAL STEP**	Check to see whether any of the transfers on the Report 22 have been tagged in ARCIS as "At Risk." If so, mark the problem on the Report 22 so that the TDS can follow up. There is no need to document a quality review error, since the transfer may have been tagged after the TDS review.	TDC or DD
7	**Check for pending or potential freezes.**	Check freeze advisories and agency communications for pending or potential freezes. If none are found, proceed to 8. If a freeze is pending or has been requested by an agency, mark the discrepancy on the Report 22. Make note of the quality review error on the appropriate QR accountability sheet.	TDC or DD

No.	Activity	Detailed Description	Responsible Party
8	**Prepare for next phase (either corrections or Director review).**	Sign and date the Report 22 to verify that you have completed all steps of your review. Did you mark any problems on the Report 22? If so, return the Report 22 and other materials to the TDS so that the TDS can make corrections. If no corrections are necessary, give the Director the following: • Report 22 (signed and dated) • NA 13001s and any supporting documents (such as freeze advisories)	TDC or DD
9	**Make and review corrections.**	**NOTE: This step is necessary only if the TDC or DD marked problems on the Report 22.** TDS: Correct all of the problems that were marked on the Report 22, then return the Report 22 and the other materials to the TDC or DD. TDC or DD: Review the corrections. If any problems remain, mark them on the Report 22 and return the materials to the TDS for additional work. Make note of the quality review error on the appropriate QR accountability sheet. If all problems have been resolved, give the marked-up Report 22, the NA	TDS and TDC/DD

No.	Activity	Detailed Description	Responsible Party
		13001s, and any supporting documents to the Director for review.	
10	**Compare transfers listed on Records Disposal Retrieval Report (Report 22) against NA 13001s.**	**NOTE: This is the third review, conducted by the Director. It is a sample check. The percentage to be reviewed is at Director's discretion.** For each of the transfers selected for review, verify that there is an NA 13001 (or its equivalent). If there is no NA 13001 (or its equivalent), mark the discrepancy on the Report 22. For each matched NA 13001, ensure that: • The "approved" block is checked • The form has been signed and dated by the authorized disposal approver If the "approved" block is not checked or the form has been signed by someone other than the authorized disposal approver, mark the discrepancy on the Report 22. Make note of the quality review error on the appropriate QR accountability sheet.	Director (D)

No.	Activity	Detailed Description	Responsible Party
11	**Check ARCIS for transfers that are "At Risk."** **THIS IS A CRITICAL STEP**	Check to see whether any of the transfers on the Report 22 have been tagged in ARCIS as "At Risk." If so, mark the problem on the Report 22 so that the TDS can follow up. There is no need to document a quality review error, since the transfer may have been tagged after the TDS review.	D
12	**Check for pending or potential freezes.**	Check freeze advisories and agency communications for pending or potential freezes. If none are found, proceed to 13. If a freeze is pending or has been requested by an agency, mark the discrepancy on the Report 22. Make note of the quality review error on the appropriate QR accountability sheet.	D
13	**Check for problems that need correction.**	Did you mark any problems on the Report 22? If so, return the Report 22 and the other materials to the TDC or DD. If no corrections are necessary, proceed to 15.	D

No.	Activity	Detailed Description	Responsible Party
14	**Make and review corrections.**	**NOTE: This step is necessary only if the Director marked problems on the Report 22.** TDC or DD: Give the Report 22 and the other materials to the TDS so that the TDS can make corrections. TDS: Correct all of the problems that were marked on the Report 22, then return the Report 22 and the other materials to the TDC or DD. TDC or DD: Review the corrections. If any problems remain, mark them on the Report 22 and return the materials to the TDS for additional work. Make note of the quality review error on the appropriate QR accountability sheet. If all problems have been resolved, give the marked-up Report 22 and the other materials back to the Director for review. D: Review the corrections. If any problems remain, mark them on the Report 22 and return the materials to the TDC or DD. Make note of the quality review error on the appropriate QR accountability sheet. If all problems have been resolved, proceed to 15.	TDS, TDC/DD, and D
15	**Return for processing.**	Sign and date the Report 22 to verify that you have completed all steps of your review. Return the Report 22 to the TDC/DD for processing.	D

Review of Physical Disposal Pulled From Shelves

No.	Activity	Detailed Description	Responsible Party
1	**Check ARCIS for transfers that are "At Risk."**	Run the ARCIS "At Risk" report every day. Check to see whether any of the transfers on the Report 22 have been tagged in ARCIS as "At Risk." If so, determine why the transfer has been tagged as "At Risk." If you are able to resolve the issue, make the necessary changes in ARCIS. Put a checkmark in the "Resolved" box and, in the Comments field, provide an explanation of how the issue was resolved. If you cannot resolve the issue, line out the transfer on the Report 22. In ARCIS, set the transfer's status back to "Shelved." The "At Risk" backlog should not exceed one month.	Transfer and Disposition Specialist (TDS)

No.	Activity	Detailed Description	Responsible Party
2	**Mark containers while still shelved.**	For each transfer that is eligible for disposal (in other words, it is listed on the Report 22 and has NOT been lined out), use a unique red mark to mark the first and last container of each contiguous run. Initial the "Marked" box on the Report 22. If there is a discrepancy, contact the TDS.	TDS or Disposition Crew Leader (DCL)
3	**Remove containers from shelving.**		

No.	Activity	Detailed Description	Responsible Party
3.1	Locate containers.	Locate the containers on the shelving, using the location information listed on the Report 22. As you locate each transfer, verify that: • The Report 22 has been initialed by the DCL. • There is a unique red mark on the first and last containers of each contiguous run. If correct, proceed to 3.2. If there is a discrepancy, contact the TDS.	Disposition Crew (DC)

No.	Activity	Detailed Description	Responsible Party
3.2	Remove containers.	Remove the containers from the shelving. As you do so, check for: • Missing and/or charged out containers • Empty locations immediately before or after a contiguous run If you find missing or charged out containers or empty locations, mark these on the Report 22. Collect any charge-out (C/O) cards to give to the TDS. Place containers on streamliners in contiguous order, facing the same direction and with transfer numbers visible (except IRS List Years, which do not need to be in contiguous order or to have numbers visible.)[1]	DC
3.3	Initial Report 22 and hand over documentation.	Each member of the DC must initial the Report 22 to verify that steps 3.1 and 3.2 have been completed. Give any C/O cards to the TDS.	DC

[1] Best practice is to identify streamliners by their current use: c.f., “disposal”; “to be shelved”; “reference”, etc.

No.	Activity	Detailed Description	Responsible Party
4	**Move records to designated disposal review area.**	Move the records to the designated disposal review area. Leave the records on the streamliners. NOTE: Only disposable records should be placed in this area.	DC
5	**Compare transfers and assets listed on Report 22 against containers pulled.**	Check every container pulled for disposal to ensure that the transfer number on the container matches the transfer number on the Report 22. (For IRS List Years, in lieu of checking the transfer number, check that the District, Tax Class, and Year are approved for disposal.) Check every eligible transfer listed on the Report 22 to ensure that every container is accounted for: either the container is there, you have a C/O card for the container, or there is an annotation on the Report 22 explaining the container's whereabouts. If a problem is discovered, immediately remove the affected container(s) from the disposal area. Make note of the quality review error on the appropriate QR accountability sheet.	TDS

No.	Activity	Detailed Description	Responsible Party
6	**Mark disposable containers.** **THIS IS A CRITICAL STEP**	Mark **EVERY** container with a red "D," or affix the ARCIS disposal label, to indicate that the container has been verified and is approved for disposal.	TDS or Quality Control Staff (QC)
7	**Palletize containers.**	Stack the records on the pallet(s). As you do so, check to ensure that: • Each container is marked with a red "D" or an ARCIS disposal label. • The containers are stacked on the pallet in container number order (to the extent practical). • The "D" marking or ARCIS disposal label is visible on the containers on the perimeter of the pallet (to the extent practical).	DC
8	**Physically check shelves for accuracy of disposal pulls.** **Note: This step is optional.**	T&D staffs should use their judgment about whether to do this step. (An example of when it might be advisable is when box markings are illegible or missing.)	TDC

No.	Activity	Detailed Description	Responsible Party
8.1	Check the shelves.	In the stacks, verify that shelves previously holding the disposable materials are in the expected state: • Spaces are empty where containers were pulled. • No additional, unanticipated empty spaces found before or after. • No containers were left behind. If the shelves appear as expected, proceed to 8.2. If errors or anomalies are found, investigate and fix them. Make note of the quality review error on the appropriate QR accountability sheet.	TDC or TDS
8.2	Sign Report 22.	Sign and date Report 22 to verify that the physical check has been completed.	TDC or TDS
9	**Prepare records for pickup.**		

No.	Activity	Detailed Description	Responsible Party
9.1	Check ARCIS for transfers that are "At Risk." THIS IS A CRITICAL STEP	Check to see whether any of the transfers on the Report 22 have been tagged in ARCIS as "At Risk." If so, determine why the transfer has been tagged as "At Risk." If you are able to resolve the issue, make the necessary changes in ARCIS. Put a checkmark in the "Resolved" box and, in the Comments field, provide an explanation of how the issue was resolved. If the transfer is no longer eligible for disposal, have the DC remove the containers from the pallet. Line out the transfer on the Report 22. In ARCIS, set the transfer's status back to "Shelved."	TDS
9.2	Ensure control of transfers	The records center must have intellectual control over pallets and the records on each pallet that are loaded on the truck.	TDC or TDS

No.	Activity	Detailed Description	Responsible Party
9.3	Load and secure the truck.	Load the disposable records onto the truck. Secure the truck and its contents using tamper evident security tape, a numerical seal and BX approved locking device. Tamper tape instructions: Place 4 strips of tamper tape on any pallet that is at an entry/exit point on the trailer - place 2 strips from the base of the pallet over in a horizontal (East/West) pattern and then place the other 2 strips from the base of the pallet in a vertical (North/South) pattern.	DC
9.4	Verify and authorize departure of truck	Verify that the truck is properly sealed and locked. That the contents are known and that all paperwork required for the truck is complete.	TDC or TDS
9.5	Update ARCIS	Once Steps 9.3 and 9.4 have been completed, the status for every transfer on the truck should be changed to Disposed in ARCIS. These actions should be completed within one workday of the truck departing the FRC	TDS
10	**File paperwork.**	File and maintain all of the documents related to this disposal cycle (including the Reports 23 and 22, the NA 13001s, all query reports, and any other documentation).	TDS

National Archives and Records Administration

Transmittal Memo

DATE: December 21, 2010

TO: Executives, Staff Directors, NHPRC, and OIG

SUBJECT: Physical Transfer of Permanent and Temporary Federal Records to NARA Records Centers for Storage and other Services

Purpose: This transmits the revised policy directive, NARA 1465, Physical Transfer of Permanent and Temporary Federal Records to NARA Records Centers for Storage and other Services.

Background/significant changes: Procedures previously included as a supplement are being incorporated into the Federal Records Center Operations Manual (formerly 'Centers 1300'), which will be made available on NARA-at-Work. Federal Records Center staff should continue to use local procedures until further notice.

Available forms:

- SF 115, Request for Records Disposition Authority
- SF 135, Records Transmittal Receipt

Canceled policy: This directive cancels NARA 1465, Physical Transfer of Permanent and Temporary Federal Records to NARA Records Centers for Storage and other Services, dated May 17, 2006.

Canceled forms: None.

Effective date: This directive is effective date of signature.

Contact information: Questions regarding this directive should be addressed to Russell F. Loiselle in Operations Branch (AFO), on (301) 837-3527 or via e-mail at Russell.Loiselle@nara.gov.

DAVID S. FERRIERO
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1465
December 21, 2010

SUBJECT: Physical Transfer of Permanent and Temporary Federal Records to NARA Records Centers for Storage and other Services

1465.1 What is the purpose of this directive?

This directive establishes NARA's internal policy for the transferring of Federal records into the physical custody of NARA records centers. These steps include, generally, reviewing SF-135s received from agencies, assigning transfer numbers, receiving transferred records from agencies, assigning space, shelving boxes, updating ARCIS, completing SF-135s, and notifying customers. (See the Federal Records Center Operations Manual for more details.)

1465.2 What are the authorities for this directive?

a. 44 U.S.C. Chapters 21, 29, 31, and 33

b. 36 CFR part 1224, Records Disposition Programs

c. 36 CFR part 1226, Implementing Disposition

d. 36 CFR part 1232, Transfer of Records to Records Storage Facilities

e. 36 CFR part 1233, Transfer, Use and Disposition of Records in a NARA Federal Records Center

1465.3 To whom does this directive apply?

This directive applies to all NARA records centers including the National Personnel Records Center and the Washington National Records Center.

1465.4 What is not covered by this directive?

This directive does not address records that have been accessioned into the National Archives of the United States (see NARA 1462, Replevin of Archival Materials). This directive also does not address records covered by the Presidential Records Act.

1465.5 Definitions of terms used in this directive

For the purpose of this directive, the following definitions apply concerning records disposition:

a. **Active records** –current records; records that are used in the day-to-day course of business.

b. **Classified records** - records that have been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure, and are marked to indicate their classified status.

c. **Contingent records** – records scheduled for the final disposition at some unspecified future time after the occurrence of a particular event.

d. **Disposition instructions** –instructions contained in a disposition agreement that mandate what is to be done with documentary material at certain points in their lifecycle. Disposition Instructions may consist of:

(1) Specification of the length of time material should be retained by their creator or custodian (a retention period);

(2) Conditions under which the creator or custodian should terminate retention;

(3) Physical or legal transfer of material to another custodian; or

(4) Destruction of records, or stipulation that material is not to be destroyed.

e. **Frozen records** – records whose scheduled disposition has been temporarily suspended because of special circumstances that affect the administrative, legal, or fiscal value of the records. Records may be "frozen" and, therefore, not eligible for destruction in the following circumstances:

(1) The agency has requested a change in the retention period for the records in accordance with 36 CFR § 1226.18;

(2) The agency notifies the particular records center that the records are needed for up to one year beyond the date they are eligible for disposal, in accordance with 36 CFR § 1226.20;

(3) NARA approves an agency's written request to extend the retention period for a series or system of records in accordance with 36 CFR § 1226.20; or

(4) Based on a Court order or request from the Department of Justice, record destruction is suspended indefinitely.

f. **Inactive records** – non-current records; records that are no longer used in the day-to-day course of business, but which may be preserved and occasionally used for legal, historical, or operational purposes.

g. **Permanent records** – any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National

Archives and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973.

h. **Records** – all books, papers, maps, photographs, machine-readable materials, 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. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included (44 U.S.C. § 3301).

i. **Temporary records** – any record which has been determined by the Archivist of the United States to have insufficient value (on the basis of current standards) to warrant its preservation by the National Archives and Records Administration. This determination may take the form of a series of records designated as disposable in

(1) An agency disposition schedule approved by NARA (SF 115); or

(2) A General Records Schedule.

j. **Transfer** – As a verb, the process supporting the moving of documentary material from one location to another. Usually used to refer to transfer of materials from the creator or custodian to NARA (including Federal records centers). As a noun, the body of documentary material being transferred.

k. **Unscheduled records** – are records the final disposition of which has not been approved by NARA.

1465.6 Responsibilities

The Federal Records Center Program has the responsibility to:

a. Receive records from Federal agencies, and the District of Columbia as warranted (per NARA 1501.6(e) (2)), for storage and provide the following services on these records prior to their final disposition: processing, holdings maintenance, preservation, and reference;

b. Provide courtesy storage for documentary materials of members of Congress;

c. Follow the transfer procedures in the Federal Records Center Operations Manual; and

d. Ensure information on the SF 135 (or electronic equivalent), Records Transmittal Receipt, is not subject to the Privacy Act (5 U.S.C § 552a) and exempt from the Freedom of Information Act (FOIA) (5 U.S.C. §552), or if it is, ensure that it is not released to the public.

1465.7 What records can agencies transfer to NARA records centers?

Agencies can transfer records that are permanent, temporary, unscheduled, active, inactive, classified, frozen, or contingent to NARA records centers. The records can be audiovisual, electronic, paper, non-paper (e.g. microfilm), or mixed media types.

1465.8 May NARA accept records subject to the Privacy Act of 1974?

Records centers may accept for storage records that are contained in a properly published Privacy Act system of records. Agencies should clearly mark the SF-135 to indicate that the records contain information covered by the Privacy Act.

1465.9 Do agency records transferred to a NARA records center remain in the legal custody of the agency?

Yes, the records remain in the legal custody of the transferring agency.

1465.10 What are NARA and agency responsibilities if an agency wants to transfer unscheduled records to NARA?

Agencies wishing to store unscheduled records at a records storage facility must notify the Office of the Chief Records Officer (AC) in writing prior to the transfer in accordance with 36 CFR § 1232.14. If receiving unscheduled Federal records for storage and other services, records center staff must verify that agency staff completing the SF 135 (or electronic equivalent) have provided the date AC was notified.

1465.11 Are SF 135s (or electronic equivalent) open to the public?

SF 135s have been open to the public since 1973 with the exception of those containing classified national security information or other information exempted from disclosure under FOIA and the Privacy Act. Records center staff must review the SF 135s (or electronic equivalent) for any information that is exempt under FOIA or the Privacy Act before providing them to a member of the public or another Federal agency.

1465.12 How are records created by this directive maintained under the NARA Records Schedule?

Maintain records created by this directive under File Nos. 1343-1 or 1343-2 as appropriate.

National Archives and Records Administration

NARA 1501
August 31, 2007

SUBJECT: Custody of Federal Records of Archival Value

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a revision of NARA 1501, Custody of Federal Records of Archival Value. The major revisions are to add Federal agencies to the lists of organizations eligible for affiliated relationship agreements with NARA and to recognize the roles of the National Records Management Program and of the Modern Records Program in supporting and development and monitoring of affiliated archives and affiliated relationships.

Cancelled directives. NARA 1501, Custody of Federal Records of Archival Value, dated February 28, 2003 is cancelled.

ALLEN WEINSTEIN
Archivist of the United States

NARA 1501
August 31, 2007

SUBJECT: Custody of Federal Records of Archival Value

1501.1 Purpose of this directive

This policy addresses the authority and responsibility of the Archivist of the United States (Archivist) regarding the physical and legal custody of Federal records "determined by the Archivist of the United States to have sufficient historical or other value to warrant their continued preservation by the United States Government" (44 U.S.C 2107(1)). This directive includes provisions for the deposit of records of archival value (designated as "permanent" on records disposition schedules) outside the physical custody of the National Archives and Records Administration (NARA).

1501.2 Authority for this directive

a. 44 U.S.C. 2107, 2108, 2109, 2111 note sec. 101(b)(2), 2112(c), 2118, 2201(2), and 2203(f)(1)

b. 36 CFR 1228.260

c. E.O. 12667

1501.3 Definitions

For the purpose of this directive, the following definitions apply.

a. **Accession** - the transfer to the Archivist of legal custody of Federal records of archival value.

b. **Affiliated archives** - a public organization, an educational institution or association, or a Federal agency that holds, by formal written agreement with NARA, physical custody of records that are accessioned into the legal custody of the National Archives and Records Administration. (This entity acts as an agent for NARA, and performs access, reference, preservation, and other archival functions – see par. 1501.10 for requirements for affiliated archives.)

c. **Affiliated relationship** - a formal association between NARA and a public organization, an educational institution or association, or a Federal agency whereby NARA and one or more other parties enter into an agreement relating to the custody of Federal records of archival value and on responsibilities for performing archival functions for those records. (Affiliated relationships include but are not limited to those with institutions that meet the requirements of being an affiliated archives – see par. 1501.12 for examples of affiliated relationships that are not affiliated archives.)

d. **Archival value** - the enduring administrative, fiscal, legal, intrinsic, historical, evidential, informational, or other research value of records, as determined by the Archivist, that warrants their continued preservation by the Government after they are no longer needed by the originating agency, or its successor in function, in the conduct of current agency business. Records determined to have archival value are designated on records disposition schedules as "Permanent records."

e. **Custody, legal** - ownership and the responsibility for creating policy governing all archival functions related to the records regardless of their physical location.

f. **Custody, physical** - the responsibility for the care of records and implementing policy governing all archival functions related to the records. (Physical custody may be, but is not always, paired with legal custody.)

g. **Federal agency** - any executive agency or any establishment in the legislative or judicial branch of the Government (except Presidential offices, the Supreme Court, the Senate, the House of Representatives, and the Architect of the Capitol and any activities under the direction of the Architect of the Capitol).

h. **Federal records** - all books, papers, maps, photographs, machine readable materials, 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).

i. **National Archives of the United States** - official records that have been determined by the Archivist to have sufficient historical or other value to warrant their continued preservation by the Federal Government, and which have been accepted by the Archivist for deposit in his custody (44 U.S.C. 2901). Hereafter, referred to as "National Archives."

j. **Originating agency** - referring to a body of Federal records, the Federal agency that originally created or received the records in the conduct of agency business.

k. **Record** - same as "Federal record" (see subpar. h).

1501.4 Holdings that are not covered by this directive

This directive does not apply to Presidential records and donated historical materials.

1501.5 Responsibilities

The Archivist (N), the Office of Regional Records Services (NR), the Office of Records Services – Washington, DC (NW), the Office of Administration (NA), and the Office of Information Services (NH) share responsibilities relating to the affiliated relationship program.

a. **The Archivist**

(1) Is responsible for the custody, use and withdrawal of records transferred to NARA.

(2) Approves the creation and termination of affiliated relationship agreements, including those for affiliated archives.

b. **NR and NW** jointly recommend to the Archivist the creation or termination of affiliated relationship agreements, including those with affiliated archives.

c. **NR**

(1) provides the lead in coordinating the affiliated relationships programs and chairs the team (consisting of NR, NW, NA, and NH) that monitors efforts.

(2) monitors the operation of affiliated archives in locations outside the Washington, DC, area.

d. **NW** monitors the operation of affiliated archives in the Washington, DC, area.

e. **NA** supports NR and NW in monitoring facility requirements; including any NARA-related signage.

f. **NH** supports NR and NW in monitoring IT requirements for electronic records.

g. **Preservation Programs (NWT)** supports NR and NW in monitoring preservation requirements.

h. **The Modern Records Program (NWM) and the National Records Management Program (NRMP)** support NR and NW in the development and monitoring of MOUs for affiliated archives and affiliated relationships with Federal agencies, including principally records management and electronic records issues.

i. **The Office of General Counsel (NGC)** participates in the development of agreements for the establishment of new affiliated relationships.

j. **The Office of Inspector General (OIG)** directs and conducts investigations as warranted related to records that have been accessioned into the legal custody of NARA.

1501.6 Transfer of custody of records with archival value

a. The Archivist determines the disposition of records. Determinations of archival value are based upon appraisal guidelines incorporated in NARA 1441, "*Appraisal Policy of the National Archives and Records Administration.*"

b. Records with archival value are transferred to the legal custody of NARA. The date of transfer is scheduled to coincide with a point at which the records are no longer needed

for the conduct of agency business (44 U.S.C. 2107 and 2901).

c. Records with archival value are also typically transferred to the physical custody of NARA. NARA accepts records in many forms, including loose papers, bound volumes, motion picture films, videotapes, sound recordings, still photographs, maps, drawings and plans, and electronic records.

d. Records that are normally transferred to the physical custody of NARA's regional archival repositories include:

(1) Records of field offices of Federal agencies, except for records of agency field offices located in the Washington, DC, area;

(2) Headquarters and field office records of agencies, such as the Tennessee Valley Authority and the Railroad Retirement Board whose headquarters are based outside of the Washington, DC, area;

(3) Modern military personnel records; and

(4) Other records determined by NARA to be of enhanced value when located with related holdings and reference experts, or nearby interested research audiences.

e. Records that are normally transferred to the physical custody of NARA's Washington, DC, area archival repositories include:

(1) Headquarters records of agencies based in the Washington, DC, area;

(2) Records relating to the District of Columbia and the Washington, DC, area; and

(3) Other records not deposited in NARA's regional archival repositories.

1501.7 When may the Archivist accelerate accessioning of records of archival value?
When the Archivist determines that records of archival value in the custody of an agency are at risk of unlawful removal, defacement, alteration, destruction, or other loss, he or she takes action to protect the records in accordance with 44 U.S.C. 2905 and may also negotiate transfer of legal and physical custody to NARA before the scheduled transfer date.

1501.8 When may the Archivist delay accessioning of records of archival value?
NARA and the originating agency agree upon the timing for accessioning the records into the National Archives. The agreement is based upon a presumption that certain conditions will be met before accessioning. If these conditions have not been met by the scheduled transfer date, the Archivist may negotiate continued custody by the agency until the conditions are met.

a. If the records are still needed for the current business of the agency, the Archivist negotiates a new accessioning date. If such records are more than 30 years old, the agency must follow the written certification requirements specified in 36 CFR 1228.264.

b. Some examples of situations in which the Archivist may delay accessioning include:

(1) Level of active retrieval for agency business purposes is too high to be managed in an archival facility; or

(2) The agency is providing specialized access services to the public that an archives does not ordinarily provide.

1501.9 What considerations affect deposit of records of archival value outside the physical custody of the National Archives and Records Administration?

Archival facilities managed by the Archivist are designed with the public interest in mind. ("Public interest" should be broadly construed to include the best interests of the public now and in the future.) In most cases it is appropriate to transfer records of archival value to one of these depositories. However, 44 U.S.C 2107(3) recognizes the possibility that the Archivist may "direct and effect, with the approval of the head of the originating agency,… the transfer of records deposited in or approved for deposit with the National Archives of the United States to public or educational institutions or associations." Such institutions, which may include Federal agencies, are called "affiliated archives." In all cases of physical deposit outside NARA, legal custody of the records remains with NARA.

1501.10 What are the criteria for establishment of affiliated archives?

Six principal criteria are used by the Archivist to determine whether it is in the public interest to establish an affiliated archives. Candidate custodians must:

a. Provide specialized public access to the records and the information in the records beyond what NARA provides. Characteristics that enable specialized access include, but are not limited to:

(1) Availability of special expertise needed to interpret the records and the recordkeeping system;

(2) Availability of special equipment or specially designed facilities needed to provide ready access to records;

(3) Possession of records, manuscripts, or other research resources that provide essential context for the records; and

(4) Close association or proximity to the segment of the public most likely to desire ready access to the records.

b. Demonstrate an institutional commitment to the long-term preservation of the records. Candidate custodians must demonstrate they have the resources to store and maintain records under preservation conditions that are at least equal to those that would be provided by NARA.

c. Demonstrate the capability to protect the information in the records in accordance with the Freedom of Information Act (FOIA), 5 U.S.C. 552 as amended. Records exempt from disclosure under the FOIA (5 U.S.C. 552) cannot be deposited outside the Federal government.

d. Agree to follow NARA reference, arrangement, description, preservation, and security guidance, including guidance on notification of NARA in the event of a theft.

e. Agree to permit NARA to examine the records and review how they are being managed, preserved, and made available for research.

f. Agree to notify NARA immediately of any substantial risk to the continued preservation of, access to, or security over the records.

1501.11 How is the decision to establish an affiliated archives documented?
The decision to establish an affiliated archives must be documented in a written agreement signed by all parties (e.g., a memorandum of understanding [MOU]). The written agreement must incorporate the criteria in par. 1501.10. The written agreement must also state that NARA retains legal custody of the records covered by the agreement and that NARA may, after providing notification and an opportunity to correct problems, take physical custody of the records if they are not maintained in accordance with the agreement. A detailed inventory of the records must be compiled as part of the MOU.

1501.12 What are examples of other affiliated relationships?
Other relationships with public organizations, educational institutions or associations, and Federal agencies are possible. Which type of affiliation to be established is at the discretion of the Archivist. Such relationships must be established by MOUs that set out the terms of the roles and responsibilities of all parties to the MOU. Examples of other possible relationships include, but are not limited to:

a. **Example 1 -** An institution holds an official copy of the record (such as a duplicating master or reference copy of microfilm or a public access copy of electronic records) and takes on access responsibilities for the record and NARA accessions and has physical custody of the preservation copy of the record.

b. **Example 2 -** NARA and other institutions may agree to cooperate in performing archival functions.

c. **Example 3 -** NARA and one or more Federal agencies may agree to cooperate to leverage their combined knowledge, expertise, and resources to assure the long-term preservation and access of specific collections of Federal records, particularly those records in special formats.

d. **Example 4** - NARA and one or more Federal agencies may agree to cooperate and provide emergency assistance to ensure records recovery.

1501.13 How are records created by this directive maintained under the NARA Records

Schedule?
Case files created during the establishment and implementation of affiliated archives and affiliated relationships are currently unscheduled. They may not be destroyed until further notice (when a disposition has been approved by the Archivist of the United States.). Some records related to policy regarding affiliated archives and affiliated relationships may be filed under 109, Program Subject Files.

National Archives and Records Administration

NARA 1502
May 31, 2005

SUBJECT: Procedures for Processing Proposals for Affiliated Archives

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a new directive establishing procedures for evaluating proposals to establish new affiliated archives.

ALLEN WEINSTEIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1502
May 31, 2005

SUBJECT: Procedures for Processing Proposals for Affiliated Archives

1502.1 What is the purpose of this directive?
This directive provides procedures for evaluating proposals to establish new affiliated archives.

1502.2 Definitions
NARA 1501, Custody of Federal Records of Archival Value, defines affiliated archives as a public or educational institution or association that holds, by formal written agreement with NARA, physical custody of records that are accessioned into the legal custody of NARA. (This entity acts as an agent for NARA, and performs access, reference, and other archival functions – see par. 1501.10 in NARA 1501 for requirements for affiliated archives.)

1502.3 Responsibilities

a. **The Archivist and Deputy Archivist (ND)**:

(1) Give preliminary and final approval or disapproval for proposals for establishment of a new affiliated archives; and

(2) Sign the memorandum of understanding (MOU) with the new affiliated archives on behalf of NARA.

b. **The Office of Regional Records Services (NR)** coordinates the review and approval process for all proposals; maintains files on the proposals and the acceptance or rejection process; maintains files on affiliated archives; and serves as NARA's primary management liaison for existing affiliated archives. The Senior Archivist for Regional and Affiliated Archives is NR's representative for affiliated archives matters.

c. **The NARA Affiliated Archives Review Team (AART)** reviews proposals for establishment of new affiliated archives and recommends approval or disapproval to NR and the Office of Records Services – Washington, DC (NW).

d. **NR and NW** jointly submit a final recommendation for approval or disapproval of a new affiliated archives to the Archivist and ND.

e. **The General Counsel (NGC)** in conjunction with the AART develops MOUs for the establishment of new affiliated archives upon final approval of the proposal.

1502.4 Where should proposals for affiliated archives be directed?

NARA units who initiate or receive proposals to become new affiliated archives must direct them
through supervisory channels within the office to NR to begin the process outlined in this directive.

1502.5 What is the first step in processing affiliated archives proposals?
NR records the proposal and forwards it to the Archivist and ND for immediate elimination of any inappropriate candidates. Processing of a proposal for a new affiliated archives may proceed only with the preliminary concurrence of the Archivist and ND. If the Archivist and ND do not give preliminary concurrence, NR prepares a response as outlined in par. 1502.12.

1502.6 When is the NARA Affiliated Archives Review Team activated?
The AART is activated when the Archivist and ND have given preliminary concurrence that a proposal for new affiliated archives may be considered. NR distributes a copy of the proposal (along with any concerns expressed by the Archivist or ND) to each member of the AART. NR convenes a meeting of the AART to consider the merits of the proposal within three weeks of its distribution.

1502.7 Who constitutes the NARA Affiliated Archives Review Team?

a. Members of the AART include:

(1) The Deputy Assistant Archivist for Records Services – Washington, DC;

(2) The Director of Archival Operations in the Office of Records Services – Washington, DC (NWA);

(3) NW's National Preservation Programs Officer for NR to provide information on the condition of the records being considered for affiliated archives status and the capabilities of the new affiliated archives to manage them to NARA standards;

(4) The Director of the Lifecycle Management Division in the Office of Records Services – Washington, DC (NWML) to provide input on the ongoing relationship with the agency records program;

(5) The Assistant for Operations in NR as the manager of the core Affiliated Archives Program;

(6) The Senior Archivist for Regional and Affiliated Archives in NR to serve as the lead for the AART and long-term management of affiliated archives;

(7) A regional archives director or NR designee (e.g., a regional administrator) to provide insight on the long-term management of the affiliated archives relationship and concerns about continuing evaluation;

(8) The Lead Program and Management Analyst in NR or designee;

(9) A representative of the Office of Administrative Services (NA) to review security and facilities issues;

(10) A representative of the Office of Human Resources and Information Services (NH) (in cases where electronic records are involved); and

(11) A representative of NGC to work with the AART on the MOU.

b. In addition to the core group identified in par. a , individual meetings of the AART will include as a full member the head of whichever NR or NW unit would have managed the Federal records if they were kept in NARA's physical custody rather than at the affiliated archives.

1502.8 How does the AART start processing affiliated archives proposals?

a. At the initial review meeting, AART members identify any information needed to complete evaluation of the proposal against NARA standards and directives. The NR representative asks the candidate affiliated archives to provide any missing or necessary information for the review, which NR forwards to AART members. Further processing of the proposal is contingent on receipt of information requested by the AART. If the AART does not identify a need for additional information to complete the evaluation, this initial review meeting will address the topics normally covered in a second meeting (see par. 1502.8b).

b. When all requested information is received from the candidate affiliated archives, NR forwards this information to AART members and convenes a second AART meeting for review. At this second meeting, AART members decide whether to recommend that NARA continue the review (e.g., hold an evaluation visit to the candidate affiliate or gather yet more information) or reject the proposal based upon the criteria established for affiliated archives in NARA 1501, par.1501.10.

1502.9 What does the AART do next if initial assessment of the proposal produces promising results?

a. Based on promising results of review of a proposal and supplementary information, NR will schedule a site visit to the candidate to include two or more AART members (or their designees). This evaluation visit involves:

(1) reviewing the building;

(2) talking to the candidate affiliate’s staff and volunteers to gauge their expertise;

(3) reviewing holdings management and reference documentation;

(4) reviewing building storage standards and holdings usage documentation;

(5) reviewing archival management and security protocols; and

(6) looking at any Federal records held by the candidate affiliate.

b. Evaluation criteria used during this candidate affiliated archives evaluation visit include criteria specified in NARA 1501, par. 1501.10, as well as applicable portions of NARA directives on:

(1) archival access procedures and reference services;

(2) arrangement and description standards and systems;

(3) loans and transportation requirements and approvals;

(4) preservation and conservation standards (including archival storage, handling, and holdings maintenance standards);

(5) requirements to meet NARA metrics reporting responsibilities; and

(6) security standards for buildings, staff, evacuation, holdings security, and reference room security, as well as information protection in accordance with the Freedom of Information Act (FOIA), 5 U.S.C. 552 as amended as codified in the law and NARA policy (e.g., NARA Directives such as NARA 1571, Archival Storage Standards).

c. Upon their return, the AART members who make a candidate affiliated archives evaluation visit send the following to NR for distribution by NR to the AART:

(1) a report of findings of the site visit at the candidate affiliated archives facility with respect to the evaluation criteria;

(2) a list of any special concerns, risks, or issues requiring further review, researching, analysis, or comment;

(3) a proposal for further action by the AART; and

(4) any useful attachments, such as forms, procedures, or policy statements.

d. NR convenes a meeting of the AART within three weeks of distribution of the site visit evaluation report. At this meeting the AART develops the group's recommendation on approval or rejection of the proposal. The AART then formulates a recommendation to NR and NW to accept or reject the proposal. If the AART cannot achieve consensus, NR will write a report summarizing the pros and cons of the proposal and the views of the individual offices.

1502.10 What issues or situations might lead the AART to recommend rejection of a proposal from a candidate affiliated archives?

Some issues that might lead the AART to recommend rejection of a candidate affiliated archives

are:

a. Lack of evidence that the repository provides:

(1) enhanced public access to the records beyond what NARA provides;

(2) access to a supplemental research audience beyond that audience that NARA ordinarily serves as is described in NARA 1501 in par. 1501.10; or

(3) a written guarantee that if the new affiliated archives should close or fail, that the affiliated archives will speedily transfer all Federal records and related finding aids and documentation back to the NARA-specified facility requested in a manner conversant with NARA shipping and transportation standards.

b. Lack of:

(1) adequate storage space;

(2) appropriately trained professional staff;

(3) appropriate transportation for loans, treatment, or copying;

(4) appropriate monitoring of storage environments and handling including researcher handling procedures;

(5) commitment to NARA's preservation or conservation standards, including holdings maintenance procedures, archival storage standards, and staff and contractor handling procedures; and

(6) public access, including reference services, service hours, copy procedures and services, appropriate citations and credit lines to NARA, and related issues.

c. Inability to meet NARA's:

(1) archival access procedures and reference services;

(2) arrangement and description standards;

(3) loans and transportation requirements and approvals;

(4) reporting requirements to meet NARA metrics responsibilities; and

(5) security standards and procedures (e.g., appropriate security systems, staffing, and protocols) as well as information protection in accordance with FOIA, 5 U.S.C. 552 as amended as codified in the law and NARA policy (e.g., NARA Directives such as NARA 1571, Archival Storage Standards).

d. Unwillingness to let NARA:

(1) inspect and evaluate the facility regularly; or

(2) inspect and evaluate the facility by the OIG for security and protection of the NARA archival records.

e. Unwillingness to report to NARA adequate, accurate, and complete metric reporting data to allow NARA to report as necessary on Federal records to Congress.

1502.11 What steps are taken to act on a recommendation of the AART?
NR's AART representative meets with NW and NR to convey the recommendation of the AART. NR's representative addresses questions raised by these office heads/staff directors, if necessary convening a meeting of the AART in order to do so. When NR and NW have reached agreement on the AART recommendation, they forward the NR/NW determination in a jointly authored memo to ND and the Archivist for approval.

1502.12 What action is taken on proposals for affiliated archives that are not approved by the Archivist?
NR's representative prepares a letter to the candidate affiliated archives for signature by the Archivist (with a copy to ND) that explains why the proposal was not approved.

1502.13 What action is taken on proposals for affiliated archives that are approved by the Archivist?

a. NR's representative consults with members of the AART (including NGC) to determine if additional information is necessary to prepare a MOU that establishes the affiliated archives. If necessary, NR's representative or their designee visits the candidate affiliate to confirm the answers to questions raised by AART review and identify any special considerations to be covered by the MOU.

b. At the end of this information-gathering phase, the AART members (or the NR representative acting as their designee) work with NGC to draft a MOU establishing the affiliated archives. The MOU must contain a requirement for regular review by NARA staffers to ensure enforcement of requirements, and inspection by NARA OIG staff relating to security and protection of the NARA holdings as needed. This MOU includes specific mention of the criteria and standards alluded to in NARA 1501, par 1501.10, including:

(1) access procedures and reference services;

(2) arrangement and description standards;

(3) loans and transportation requirements and approvals;

(4) preservation and conservation standards (including archival storage

standards);

(5) reporting requirements to meet NARA metrics responsibilities; and

(6) security standards as well as information protection in accordance with FOIA, 5 U.S.C. 552 as amended.

c. NR's representative:

(1) Drafts a letter for the Archivist's signature to enclose the MOU for forwarding to the candidate affiliated archives; and

(2) Prepares a NARA Notice announcing the establishment of the affiliated archives.

1502.14 How are records created by this directive maintained under the NARA records schedule?

Records created for the processing of proposals, including records of the AART, are currently unscheduled. Responsible offices and the AART must not destroy any records created by this directive until the Archivist approves dispositions on an SF 115, Request for Records Disposition Authority.

National Archives and Records Administration

NARA 1603
June 23, 2006

SUBJECT: Access to Records under the Privacy Act

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a directive on how to process requests for access to and amendments of records subject to the Privacy Act of 1974, as amended, (5 U.S.C. 552a).

Significant changes

- Par. 1603.7 -Applicability section which made reference to administrative records, changed to operational records consistent with our implementing regulations

- Pars. 1603.6 and 1603.15 – 1603.16 - Registering request - entire section has been revised to direct change in policy and staff designations

- Clearance of Responses and Signatory levels have been removed because they are not applicable

- Pars 1603.35 – 1603.37 - Creating new systems revised to reflect current practice and appropriate staff organizations

- Updated appendices concerning NARA systems consistent with the latest Federal Register publication. Added a new appendix for Government –wide Systems

- Updated inventory of system managers and facilities to reflect current office designations and facility addresses

Canceled directives. This directive cancels

- ADMIN. 201 – Chapter 1. General – Part 6. Privacy Act
- Interim Guidance 1600-2, Use of NARA's Privacy Systems for Investigations, dated November 20, 2001

ALLEN WEINSTEIN
Archivist of the United States

Attachment

National Archives and Records Administration

NARA 1603
June 23, 2006

SUBJECT: Access to Records under the Privacy Act

1603.1 What is the purpose of this directive?

This directive

a. Provides policy and procedures on how to process requests for access to and amendments of records subject to the Privacy Act of 1974, as amended, (5 U.S.C. § 552a), hereafter referred to as the Privacy Act.

b. Describes the process for publishing a new or revised Privacy Act system of records; and,

c. Transmits lists of:

(1) NARA's Privacy Act Systems of Records (appendix A);

(2) Routine uses for access to records under the Privacy Act (appendix B);

(3) Privacy Act systems exempt from disclosure (appendix C);

(4) NARA system managers (appendix D); and

(5) Government-wide system notices for common records (appendix E).

1603.2 Authority for this directive

a. 5 U.S.C. § 552a, as amended;

b. 44 U.S.C. § 2104(a); and

c. 36 CFR part 1202.

1603.3 Applicability

This directive applies to records subject to the provisions of the Privacy Act of 1974, as amended.

1603.4 What is the difference between the Privacy Act and the Freedom of Information Act (FOIA)?

a. The Privacy Act, among other things, allows United States citizens or lawfully admitted permanent residents to gain access to name-retrievable information that is maintained on themselves in a system of records, unless such information is exempt from disclosure.

b. FOIA, as amended (5 U.S.C. § 552), allows any person the right to gain access to records created or maintained by an executive branch agency unless such information is exempt from disclosure under one or more of the FOIA's nine exemptions.

1603.5 Definitions

The following definitions apply to terms used in this directive:

a. **Access** - the transfer of a record, a copy of a record, or the information in a record to the subject individual, or the review of a record by the subject individual.

b. **Agency** - any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

c. **Defunct agency records** - records in a Privacy Act system of a defunct agency that are stored in a NARA records center.

d. **Disclosure** - the transfer by any means of a record, a copy of a record, or the information contained in a record to a recipient other than the individual who is the subject of the record, or the review of a record by someone other than the subject individual.

e. **Individual** - a citizen of the United States or an alien lawfully admitted for permanent residence.

f. **Maintain** - to file, collect, use, or disseminate information.

g. **Record subject to the Privacy Act** - any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history and criminal or employment history, and that contains his or her name or an identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint, or photograph. For purposes of this directive, "record" does not mean archival records that have been transferred to the National Archives of the United States.

h. **Routine use** - with respect to the disclosure of a record, the use of that record for a purpose which is compatible with the purpose for which it was collected.

i. **Subject individual** - the individual named or discussed in a record or the individual to whom a record pertains.

j. **System manager** - the NARA official who is responsible for the maintenance of a system of records and for the collection, use, and dissemination of information in that system of records (see appendix D).

k. **System of records** - a group of records under the control of NARA from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to that individual. Records about individuals are not part of a system of records if they are maintained chronologically or in another filing scheme not based on retrieval by personal identifier.

1603.6 What are NARA's responsibilities under the Privacy Act?

a. **Privacy Act system managers** (see appendix D) are responsible for:

(1) Ensuring that name retrievable information, in a system of records, is accurate, relevant, complete and up-to-date before disclosing it to others;

(2) Processing, in conjunction with the NARA Privacy Act Officer, requests for access to and amendments of records subject to the Privacy Act;

(3) Ensuring that the appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of records subject to the Privacy Act;

(4) Ensuring any disclosures are made only as allowed by the routine uses outlined in the system of records from which the records were retrieved and in accordance with this directive and NARA's implementing Privacy Act regulations; and,

(5) Maintaining an accurate accounting of disclosures, except in the case of exempt systems.

b. **NARA Privacy Act Officer** (hereafter 'Privacy Act Officer') in the Office of General Counsel (NGC) is responsible for:

(1) Ensuring NARA's compliance with the requirements of the Privacy Act and for serving as the point of contact for the public on Privacy Act requests and information;

(2) Ensuring that forms used to collect information that is maintained in a system of record contain or are accompanied by a Privacy Act disclosure statement;

(3) Maintaining the log of Privacy Act requests received by NARA;

(4) Ensuring that all NARA employees and contractors involved in the design, development, operation or maintenance of any system of records, review the provisions of the Privacy Act and its implementing regulations; and,

(5) Preparing Privacy Act and Computer Matching Reports to Congress and the Office of Management and Budget once every two years with input from NARA system managers.

c. **The Archivist of the United States** is NARA's appeal official for all access and amendment requests under the Privacy Act denied by the Inspector General (OIG) (see 36 CFR 1202.56(a)(1) and 1202.80(a)(2)). Determinations are made within 30 work days from the date on which the appeal is received.

d. **The Deputy Archivist of the United States** is NARA's appeal official for all access and amendment requests under the Privacy Act denied by other NARA offices (see 36 CFR 1202.56(a)(2) and 1202.08(a)(1)). Determinations are made within 30 work days from the date on which the appeal is received.

e. For current NARA employees seeking amendment of records maintained in the employee's Official Personnel Folder or in another Government-wide system maintained by NARA on behalf of another agency, the Privacy Act Officer provides the employee with the name and address of the appropriate appeal official in that agency.

1603.7 What records are covered by this directive?

This directive applies to NARA operational records (records used in current NARA business) and non-accessioned records of any defunct agency that are stored in a NARA records center and that are explicitly covered by the defunct agency's Privacy Act system of records. Accessioned records are specifically excluded from the provisions of the Privacy Act (see para. 1603.8).

1603.8 What records are not covered by this directive?

a. This directive specifically excludes records that have been transferred to NARA for permanent retention.

b. Presidential records, records covered by the Presidential Recordings and Materials Preservation Act, and donated historical materials are specifically excluded from the provisions of the Privacy Act.

c. Records of other agencies that are stored in Federal records centers are governed by the Privacy Act rules of the originating agency.

d. Personnel and medical records held by the National Personnel Records Center (NPRC) on behalf of the Department of Defense and the Office of Personnel Management (OPM) are subject to the Privacy Act regulations of those agencies.

e. Requests for disclosure of publicly-available information such as official position descriptions, title, grade and salary of agency employees are processed under the provisions of FOIA (see NARA 1602, Access to Records Requested under FOIA).

1603.9 Does the Privacy Act limit NARA's ability to compile names and addresses for mailing lists?

The Privacy Act places limitations on the use of mailing lists. Consult with the Privacy Act Officer before establishing a new mailing list or before renting, exchanging, or selling an existing mailing list. The Privacy Act Officer ensures that the proposed mailing list is covered by an existing Privacy Act system or that the proposed use of the mailing list complies with the provisions of the Privacy Act.

1603.10 How does NARA collect information about individuals?

To ensure that information maintained on individuals is accurate, timely and correct, NARA collects information directly from the individual to the greatest extent possible.

1603.11 What information does NARA provide to an individual before collecting information using NARA forms?

a. System managers, in conjunction with the Privacy Act Officer, ensure that forms used to record information provided by individuals comply with the provisions of the Privacy Act and Office of Management and Budget requirements. See NARA 108, Information Collection, for procedures on developing and obtaining approval on information collections.

b. Once appropriate clearance has been granted for an information collection, system managers or designated agency employees must provide the individual with a Privacy Act disclosure statement that includes the following elements:

(1) The authority (statute or Executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(2) The principal purpose(s) for which the information will be used;

(3) The routine uses (see appendix B) that may be made of the information. Consult the Privacy Act Officer to ensure that these routine uses have been included in the system of records notice published in the Federal Register; and,

(4) The effects on the individual who supplies the information, if any, for not providing all or any part of the requested information.

1603.12 Who can request access to records under the Privacy Act?

A citizen of the United States or an alien lawfully admitted for permanent residence can file a request for access to records about themselves under the provisions of the Privacy Act. Requests from other individuals and agencies for records in a Privacy Act system are handled in accordance with pars. 1603.17 through 18 and 1603.26.

1603.13 How do these individuals gain access to records about themselves?

All requests for records contained in a NARA Privacy Act system of records must be made in writing and sent to the Privacy Act Officer. The Privacy Act Officer ensures that the information required by 36 CFR 1202.40 (for access by subject individuals) and 36 CFR 1202.62 (for disclosure to third parties) is provided.

1603.14 Can the subject authorize a third party to gain access to his or her records?

The subject of a record can authorize another individual to have access to his or her record. The subject individual's request must identify the authorized third party and be accompanied by proof of identity as outlined in 36 CFR 1202.40.

1603.15 Who processes requests for access to information under the Privacy Act?

a. All Privacy Act requests are processed by the appropriate NARA system manager in coordination with the Privacy Act Officer. When an office receives a Privacy Act request for a NARA operational record or a record of a defunct agency in a NARA records center, the office must notify the Privacy Act Officer before taking any action.

b. The Inspector General (OIG) processes Privacy Act requests for investigative records. OIG may consult with the Privacy Act Officer or other officials as necessary.

1603.16 How are Privacy Act requests processed for disclosure?

Upon receipt of a Privacy Act request the Privacy Act Officer logs the request and forwards the request to the appropriate system manager(s) for processing. The system manager, in

consultation with the Privacy Act Officer determines access rights in accordance with the provisions of the Privacy Act and the applicable system of records notice. The system manager informs the requester, in writing, of the final determination and appropriate appeal rights.

1603.17 When does NARA disclose a record in a Privacy Act system of records to an individual other than the subject of the records (third party access)?

No record in a system of records may be disclosed to any person or any agency without the express written consent of the subject individual unless the disclosure meets one of the conditions for disclosure without consent as provided for in 5 U.S.C. 552a(b). Those reasons are:

a. Disclosure to NARA employees who have a need for the information in the performance of their official duties.

b. Disclosure required under FOIA (5 U.S.C. 552).

c. Disclosure in accordance with a published routine use (NARA's general routine uses are listed in appendix B and additional routine uses are published in the individual NARA Privacy Act system of records notice).

d. Disclosure to the Bureau of the Census for uses described in 13 U.S.C.

e. Disclosure to a recipient who has provided NARA with advance adequate written assurance that the records will be used solely as a statistical research or reporting record.

f. Disclosure to NARA as a record that has sufficient historical or other value to warrant its permanent preservation.

g. Disclosure to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, if the activity is authorized by law and if the head of the agency or instrumentality has made a written request to NARA specifying the particular portion desired and the law enforcement activity for which the record is sought.

h. Disclosure to a person showing compelling circumstances affecting the health or safety of an individual. Upon such disclosure, a notification must be sent to the last known address of the subject individual.

i. Disclosure to either House of Congress or to a subcommittee or committee (Joint

or of either House, to the extent that the subject matter falls within its jurisdiction).

j. Disclosure to the Comptroller General or any authorized representatives in the course of the performance of the duties of the Government Accountability Office.

k. Disclosure to a consumer reporting agency (credit bureau) when trying to collect a claim of the Government in accordance with § 3711(f) of 31 U.S.C.

l. Disclosure is required by a court order signed by a judge.

1603.18 What are the procedures for disclosure of records to a third party?
Requests may be made by individuals or organizations for information from or copies of records pertaining to other individuals that are contained in a Privacy Act system of records. System managers must:

a. Not disclose a record in a system of records to any person or agency without the express written consent of the subject individual unless the disclosure meets one of the conditions described in para. 1603.17;

b. Treat third party requests for access as a FOIA request and apply appropriate FOIA exemptions before Privacy Act provisions are applied. See NARA 1602, "Access to Records Under the Freedom of Information Act (FOIA)," for additional information on applying FOIA exemptions; and

c. Consult with the Privacy Act Officer for the routine uses applicable to a specific system.

1603.19 How does the system manager handle requests for access to medical records under the provisions of the Privacy Act?

a. If a system manager receives a request for access to a medical record covered by this directive, the request must be forwarded to the Privacy Act Officer. If the Privacy Act Officer believes that the disclosure of the medical and/or psychological information directly to the subject may have an adverse effect, NARA asks the subject to designate in writing a physician or mental health professional to whom the records should be disclosed.

b. The OIG makes determinations concerning access to medical records for which the OIG is the system manager.

1603.20 What are the time limits for processing a Privacy Act request?

a. System managers must acknowledge a request within 10 work days of its receipt by NARA and, if possible, make the records available in that same time period.

b. If the system manager cannot make the records available within 10 work days of receiving the request, the system manager must notify the requester of the delay and provide a date when the records can be made available.

1603.21 How does a system manager provide access to Privacy Act records?

After consulting with the Privacy Act Officer, the system manager provides photocopies of the requested records by mail or provides access to the requested records during normal business hours at the NARA facility where the records are located. If the person picks up the records in-person, proof of identity, as described in 36 CFR 1202.40, is required at the time of pick-up. The proof of identity furnished with the request serves as verification of the identity of the individual when the system manager sends Privacy Act protected records through the mail.

1603.22 What fees are associated with all Privacy Act requests and what are the payment procedures?

a. NARA generally waives the fees for the first 100 pages copied or when the cost to collect the fee exceeds the amount collected. After the first 100 pages NARA charges $0.20 per page if NARA staff makes the copies or $0.15 per page if the copies are made on a self-service copier. NARA does not charge search or review fees in conjunction with Privacy Act requests.

b. Fees for reproductions of Privacy Act records can be paid by check or money order made payable to the National Archives and Records Administration or NARA. All payments should be addressed to the Privacy Act Officer in NGC.

1603.23 On what grounds can NARA deny a Privacy Act request?

a. A system manager may deny a request for access only if:

(1) NARA has published rules in the Federal Register exempting the pertinent system of records from the access requirement (NARA's exempt systems are identified in appendix C); and

(2) The record is exempt from disclosure under FOIA.

b. When NARA receives a request for access to a record that is contained in an exempt system of records, the system manager, with appropriate coordination with the Privacy Act Officer, must:

(1) Review the record to determine if all or part of the record must be withheld; and,

(2) Provide access to the releasable portions of the record consistent with para. 1603.21.

c. If a Privacy Act request is denied in whole or in part, the system manager must inform the requester in writing which Privacy Act and FOIA exemptions apply and inform the requester of his or her appeal rights. An informational copy of the denial must be sent to the Privacy Act Officer.

1603.24 How do requesters appeal denials of requests?

A requester who is denied access in whole or in part to a record subject to the Privacy Act has the right to file an appeal of that denial. The appeal letter must be postmarked no later than 35 calendar days after the date on the denial letter from NARA. Appeals are adjudicated by the appropriate NARA official as designated in para. 1603.6(c) or (d).

1603.25 How are appeals under the Privacy Act processed and what other recourse is available to requesters?

a. Upon receipt of a Privacy Act appeal, the designated NARA Privacy Act appeal official consults with the system manager, NGC, and other NARA officials as appropriate. If it is determined that the requested records are not exempt from disclosure the records are released and the requester is notified of the disclosure in writing.

b. If, after consultation with the appropriate staff, the designated NARA Privacy Act appeal official determines that the records are not appropriate for disclosure, the appeal official will notify the requester in writing of that determination. The letter will include:

(1) The reason for the denial of the appeal; and

(2) Notice of the right to seek judicial review of NARA's final determination.

c. The appeal official will make the final determination within 30 work days from the date on which the appeal is received. If the appeal official cannot make a decision within the designated time limit, he or she will notify the requester in writing and provide an explanation concerning the delay.

1603.26 How are third party appeals for access processed?

Appeals of denials of third party requests under the Privacy Act are processed, under both FOIA

and the Privacy Act, consistent with the provisions outlined in paras. 1603.24 and 1603.25.

1603.27 What are the procedures for allowing an individual to conduct statistical research among Privacy Act protected records?

a. NARA may consider requests for the sole purposes of conducting statistical research. If the requester requests access for statistical research, the written request must include the following information:

(1) A statement or the purpose for requesting the records; and,

(2) The requester has to assure NARA, in writing, that the records will be used for statistical purposes.

b. The appropriate system manager, in consultation with the Privacy Act Officer, will make a determination on whether or not to disclose records for the statistical research project within 10 work days and make a final decision within 30 work days unless NARA notifies the requester of a delay in processing.

c. If the system manager decides to deny the request, he or she notifies the requester in writing and informs of the right to file an administrative appeal to the appropriate NARA Privacy Act appeal official.

d. If the system manager approves the request for disclosure for a statistical research project, the system manager ensures that personal identifying information is deleted from the record released for statistical purposes and that the identity of the individual cannot reasonably be deduced by combining various statistical records.

1603.28 How does a system manager keep an accounting of disclosures under the Privacy Act?

a. Except for disclosures made to NARA employees in the course of performing their official duties or as required by the Freedom of Information Act (see paras. 1603.17), the system manager keeps an accurate accounting of each disclosure under the Privacy Act. The accounting includes:

(1) Date of disclosure:

(2) Nature and purpose of each disclosure; and

(3) Name and address of the person or agency to which disclosure was made.

b. The system manager also maintains with the accounting of disclosures:

(1) A full statement of the justification for the disclosures;

(2) All documentation surrounding disclosure of a record for statistical or law enforcement purposes; and

(3) Evidence of written consent by the subject individual to a disclosure, if applicable.

c. Accounting of disclosures will be made available to the subject individual upon request, except for the accounting of disclosures made for a law enforcement activity or of disclosures made from an exempt system.

d. The system manager must retain the accounting of disclosure for five years after the disclosure or for the life of the record, whichever is longer.

1603.29 Does an individual have the right to request the amendment of inaccurate information under the Privacy Act?

Yes, an individual has the right to request that his or her record be amended. If an individual determines that a record NARA maintains on them is not accurate, he or she has the right to request that the record be amended. The Privacy Act requires that agencies maintain records that are accurate, timely, relevant, and complete.

1603.30 Who handles requests for amendments under the Privacy Act?

Requests for amendments are sent to the Privacy Act Officer, in NGC, and routed to the appropriate system manager, except:

a. The OIG processes requests for amendments for records for which the OIG is the system manager.

b. NARA employees who wish to amend records in their official personnel folders must write to the Chief Human Capital Officer (H).

1603.31 What must requests for amendments include?

Requests for amendments should provide as much information, documentation, or other evidence

as needed to support the request for an amendment. Requests for amendments should contain the same identifying information as outlined in 36 CFR 1202.40.

1603.32 How does NARA handle requests to amend records?

a. The Privacy Act Officer or the Inspector General, for Privacy Act records held by OIG, in coordination with the appropriate system manager, processes requests to amend a record within 10 work days of receipt. The response letter from the NARA Privacy Act Officer of the Inspector General will include the system manager's determination to either amend the record or deny the request.

b. If the Privacy Act Officer or OIG, as appropriate, approves the amendment request, he or she will direct the system manager to make the necessary amendment to the record and will send a copy of the amendment to the subject of the record.

c. The system manager will inform all previous recipients of the record, using the accounting of disclosures that an amendment has been made and give the substance of the amendment. The system manager will provide copies of the amended records where practicable.

1603.33 What happens if the Privacy Act Officer, OIG, or appropriate system manager denies a request for an amendment?

If the Privacy Act Officer, OIG, or appropriate system manager denies a request to amend a record or determines that the record should be amended in a manner other than requested by the subject, the Privacy Act Officer, OIG, or appropriate system manager will advise of that decision in writing. The denial letter will include:

a. The reason for the denial of the amendment request;

b. Proposed alternative amendments, if appropriate;

c. The subject's right to appeal the denial; and

d. The procedures for appealing the denial.

1603.34 What are the requester's options if the request to amend a record is denied?

a. If the requester agrees to accept an amendment to a Privacy Act record other than the amendment proposed in the request, the requester must notify the Privacy Act Officer in writing. Upon confirmation, the Privacy Act Officer will make the necessary amendments to the record.

b. For current NARA employees, if the denial to amend concerns a record maintained in the employee's Official Personnel Folder or in another Government-wide system maintained by NARA on behalf of another agency, the Privacy Act Officer will provide the employee with the name and address of the appropriate appeal official in that agency.

c. If the requester disagrees with the denial of a request to amend a record, he or she may file an appeal consistent with the provisions outlined in paras. 1603.24 and 1603.25.

d. If a requester is not satisfied with the result of an appeal, he or she may:

(1) Seek judicial review, or

(2) File a statement of disagreement with the appropriate system manager. The statement of disagreement must include an explanation of why the requestor believes the record to be inaccurate, irrelevant, untimely, or incomplete. The system manager will maintain the statement of disagreement in conjunction with the pertinent record. If applicable, the system manager will send a copy of the statement of disagreement to any person or agency to whom the record has been disclosed.

1603.35 What is the process for establishing or revising a system of records notice?

New and revised systems of records must be reviewed by OMB and Congress, and a notice must be published in the Federal Register before the systems can go into effect. When an office believes that a new or revised Privacy Act system is needed, the office head or staff director must consult the Privacy Act Officer.

1603.36 How is a Privacy Act systems of records developed and sent for publication?

a. A proposal for a new or revised system of records must be sent through office channels to the Privacy Act Officer at least 90 days before any new or revised system of records can go into effect. The proposal must include a complete description of and justification for each new or altered records system.

b. The Privacy Act Officer, in conjunction with the system manager, NGC, and the Strategy Division (SP), prepare the Privacy Act system notice and transmit the notice of the proposed establishment or alteration of a system of records for publication in the Federal Register. The system notice is signed by the Archivist. When the review and comment period is completed, the Privacy Act Officer notifies the system manager that the new or revised system can be implemented.

1603.37 What does a Privacy Act systems of records notice contain?

A Privacy Act system of records notice contains the following elements:

a. The system notice identifier;

b. The title of the system;

c. The location(s) of the records;

d. The individuals on which information is being collected;

e. The kinds of records being maintained in the file;

f. The authority allowing for the collection of information;

g. The purpose for collecting the information and who within NARA will have access;

h. The identities of those outside NARA who can have access to the information and for what purpose (routine uses);

i. How the records will be stored (electronically, manually, etc.);

j. How the records are retrieved (To be a Privacy Act system of record, the information must be retrieved by an individual's name or personal identifier);

k. The safeguards in place to protect unauthorized access to this information;

l. The retention and disposal requirements that will be followed for the records;

m. The systems manager;

n. The procedures for gaining access to the records; how to file a request; and how to contest the contents of the file;

o. Where the information is received from; and

p. The material in the record that can be released.

1603.38 How do system managers safeguard records in a system of records?

The system manager ensures that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of records. In order to protect against any threats or hazards to their security or loss of integrity, paper records are maintained in areas accessible only to authorized NARA personnel. Electronic records are accessed via passwords from terminals located in attended offices. After hours, doors are secured and entrances are monitored by electronic surveillance equipment or security guards.

1603.39 What are the record keeping requirements for access to or disclosure of Privacy Act records?

Records maintained in NARA's Privacy Act systems are managed in accordance with the instructions in the NARA records schedule contained in FILES 203, the NARA Files Maintenance and Records Disposition Manual.

a. The Office of General Counsel (NGC) maintains records under the file number 1103-6a and -6b, as appropriate.

b. All other offices maintain records under file numbers 1014 through 1020, as appropriate.

Appendix A - NARA Privacy Act systems of records

System Number	System Name
NARA 1	Researcher Application Files
NARA 2	Reference Request Files
NARA 3	Donors of Historical Materials Files
NARA 4	Committee and Foundation Member Files
NARA 5	Conference, Workshop, and Training Course Files
NARA 6	Mailing List Files
NARA 7	Freedom of Information Act (FOIA) Request Files and Mandatory Review of Classified Documents Request Files
NARA 8	Restricted and Classified Records Access Authorization Files
NARA 9	Author Files
NARA 10	**RESERVED**
NARA 11	Credentials and Passes Files
NARA 12	Emergency Notification Files
NARA 13	Defunct Agency Records
NARA 14	Payroll and Time and Attendance Reporting System Records
NARA 15	Freelance Editor/Indexer Files
NARA 16	Library Circulation Files
NARA 17	Grievance Records
NARA 18	General Law Files
NARA 19	Worker Compensation Files
NARA 20	Reviewer/Consultant Files
NARA 21	Fellowship and Editing Institute Application Files
NARA 22	Employee Related Files

NARA 23	Investigative Case Files
NARA 24	Personnel Security Files
NARA 25	Order Fulfillment and Accounting System Records
NARA 26	Volunteer Files
NARA 27	Contracting Officers and Contracting Officer's Technical Representative Designation Files
NARA 28	Tort and Employee Claims Files
NARA 29	State Historical Records Advisory Board Member Files
NARA 30	Garnishment Files
NARA 31	Ride Share Locator Database
NARA 32	Alternative Dispute Resolution Files
NARA 33	Development and Donor Files
NARA 34	Agency Ethics Program Files
NARA 35	Case Management System (NPRC)
NARA 36	Transportation Benefit Program Files
NARA 37	Order On-line!
NARA 38	Project Management Records

Appendix B – NARA routine uses

The following routine use statements apply to National Archives and Records Administration Privacy Act Systems of Records notices where indicated:

A. Routine Use-Law Enforcement: In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records, may be referred, as a routine use, to the appropriate agency, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

B. Routine Use-Disclosure When Requesting Information: A record from this system of records may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal or other relevant enforcement information or other pertinent information, such as current licenses, if necessary, to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

C. Routine Use-Disclosure of Requested Information: A record from this system of records may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, conducting a security or suitability investigation, classifying a job, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on

the matter.

D. Routine Use-Grievance, Complaint, Appeal: A record from this system of records may be disclosed to an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee. A record from this system of records may be disclosed to the United States Office of Personnel Management, the Merit Systems Protection Board, Federal Labor Relations Authority, or the Equal Employment Opportunity Commission when requested in the performance of their authorized duties. To the extent that official personnel records in the custody of NARA are covered within the system of records published by the Office of Personnel Management as Government wide records, those records will be considered as a part of that Government-wide system. Other records covered by notices published by NARA and considered to be separate systems of records may be transferred to the Office of Personnel Management in accordance with official personnel programs and activities as a routine use.

E. Routine Use-Congressional Inquiries: A record from this system of records may be disclosed as a routine use to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the request of the individual about whom the record is maintained.

F. Routine Use-NARA Agents: A record from this system of records may be disclosed as a routine use to an expert, consultant, agent, or a contractor of NARA to the extent necessary for them to assist NARA in the performance of its duties. Agents include, but are not limited to, GSA or other entities supporting NARA's payroll, finance, and personnel responsibilities.

G. Routine Use-Department of Justice/Courts: A record from this system of records may be disclosed to the Department of Justice or in a proceeding before a court or adjudicative body before which NARA is authorized to appear, when: (a) NARA, or any component thereof; or, (b) any employee of NARA in his or her official capacity; or, (c) any employee of NARA in his or her individual capacity where the Department of Justice or NARA has agreed to represent the employee; or (d) the United States, where NARA determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or by NARA before a court or adjudicative body is deemed by NARA to be relevant and necessary to the litigation, provided, however, that in each case, NARA determines that disclosure of the records is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

Appendix C – NARA Privacy Act systems exempt from disclosure

The following NARA systems of records are exempt from disclosure:

a. NARA 23 - Investigative Case files and

b. NARA 24 - Personnel Security Case Files.

These systems of records are exempt:

a. To the extent that the systems of records consist of investigatory material compiled for law enforcement purposes; however, if any subject individual is denied any right, privilege, or benefit to which the individual would otherwise be eligible as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 30, 1975, under an implied promise that the identity of the source would be held in confidence; and

b. To the extent the systems of records consist of investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 30, 1975, under an implied promise that the identity of the source would be held in confidence.

Appendix D - NARA Privacy Act system managers

To inquire about a Privacy Act request or to gain access to your records, requests should be submitted in writing to:

NARA Privacy Act Officer
Office of General Counsel
National Archives at College Park
8601 Adelphi Road, Room 3110
College Park, MD 20740-6001

If the system manager is the Executive for Research Services,
the records are located at the following address:

Executive for Research Services National Archives at College Park
8601 Adelphi Road, Room 3400
College Park, MD 20740-6001

If the system manager is the director of a Presidential Library, the records are located at the appropriate Presidential Library, Staff or Project:

GEORGE BUSH LIBRARY
1000 George Bush Drive West
College Station, TX 77845

JIMMY CARTER LIBRARY
441 Freedom Parkway
Atlanta, GA 30307-1498

WILLIAM J. CLINTON PRESIDENTIAL LIBRARY

1200 President Clinton Avenue
Little Rock, AR 72201

DWIGHT D. EISENHOWER LIBRARY
200 SE 4th Street
Abilene, KS 67410-2900

GERALD R. FORD LIBRARY
1000 Beal Avenue
Ann Arbor, MI 48109-2114

HERBERT HOOVER LIBRARY
210 Parkside Drive
P.O. Box 488
West Branch, IA 52358-0488

LYNDON B. JOHNSON LIBRARY
2313 Red River Street
Austin, TX 78705-5702

JOHN F. KENNEDY LIBRARY
Columbia Point
Boston, MA 02125-3398

NIXON PRESIDENTIAL MATERIALS STAFF
National Archives at College Park
8601 Adelphi Road
College Park, MD 20740-6001

RONALD REAGAN LIBRARY
40 Presidential Drive
Simi Valley, CA 93065-0600

FRANKLIN D. ROOSEVELT LIBRARY
4079 Albany Post Road
Hyde Park, NY 12538-1999

HARRY S. TRUMAN LIBRARY
500 West U.S. Highway 24
Independence, MO 64050-1798

PRESIDENTIAL MATERIALS STAFF
National Archives and Records Administration
700 Pennsylvania Ave, NW
Washington, DC 20408

OFFICE OF PRESIDENTIAL LIBRARIES
National Archives at College Park
8601 Adelphi Road, Room 2200
College Park, MD 20740-6001

If the system manager is the director of a Regional Records Center or Regional Archives facility, the records are located at the appropriate Regional Records Center or Regional Archives Facility:

NARA's Pacific Alaska Region (Anchorage)
654 West Third Avenue
Anchorage, Alaska 99501-2145

NARA's Southeast Region (Atlanta)
5780 Jonesboro Road
Morrow, Georgia 30260

NARA's Northeast Region (Boston)
Frederick C. Murphy Federal Center
380 Trapelo Road
Waltham, Massachusetts 02452-6399

NARA's Great Lakes Region (Chicago)
7358 South Pulaski Road
Chicago, Illinois 60629-5898

NARA's Great Lakes Region (Dayton)
3150 Springboro Road
Dayton, Ohio 45439-1883

NARA's Rocky Mountain Region (Denver)
Bldg. 48, Denver Federal Center
P. O. Box 25307
West 6th Avenue and Kipling Street
Denver, Colorado 80225-0307

NARA's Southwest Region (Fort Worth)
501 West Felix Street, Building 1
Fort Worth, Texas 76115-3405

NARA's Central Plains Region (Kansas City)
2312 East Bannister Road
Kansas City, Missouri 64131-3

NARA's Pacific Region (Laguna Niguel, CA)
24000 Avila Road, 1st Floor, East Entrance
Laguna Niguel, California 92677-3497

NARA's Central Plains Region (Lee's Summit, MO)
200 Space Center Drive
Lee's Summit, Missouri 64064-1182

NARA's Northeast Region (New York City)
201 Varick Street
New York, New York 10014-4811

NARA's Mid Atlantic Region (Center City Philadelphia)
900 Market Street
Philadelphia, Pennsylvania 19107-4292

NARA's Mid Atlantic Region (Northeast Philadelphia)
14700 Townsend Road
Philadelphia, Pennsylvania 19154-1096

NARA's Northeast Region (Pittsfield, MA)
10 Conte Drive
Pittsfield, Massachusetts 01201-8230

NARA's Pacific Region (San Francisco)
1000 Commodore Drive
San Bruno, California 94066-2350

NARA's Pacific Alaska Region (Seattle)
6125 Sand Point Way NE
Seattle, Washington 98115-7999

National Personnel Records Center

Civilian Personnel Records
111 Winnebago Street
St. Louis, Missouri 63118-4126

National Personnel Records Center
Military Personnel Records
9700 Page Avenue
St. Louis, MO 63132-5100

Washington National Records Center
4205 Suitland Road,
Suitland, MD 20746-8001

If the system manager is the Executive Director of the National Historical Publications and Records Commission (NHPRC), the records are located at the following address:

National Historical Publications and Records Commission
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

If the system manager is the Chief Strategy and Communications Officer, the records are located at the following address:

Strategy and Communications Office (
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

If the system manager is the Director of Congressional Affairs, the records are located at the following address:

Congressional Affairs Staff
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

If the system manager is the Executive for Information Services, the records are located at the following address:

Information Services

National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740

If the system manager is the Executive for Business Support Services, the records are located at the following address:

Business Support Services
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740

If the system manager is the Director of the Federal Register, the records are located at the following address:

Office of the Federal Register
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

If the system manager is the Inspector General, the records are located at the following address:

Office of the Inspector General
National Archives and Records Administration
8601 Adelphi Road, Room 1300
College Park, MD 20740

If the system manager is the General Counsel, the records are located at the following address:

Office of the General Counsel
National Archives and Records Administration
8601 Adelphi Road, Room 3110
College Park, MD 20740

Appendix E – Government-wide Privacy Act systems of records maintained by NARA

Note: This is not a comprehensive list of the Government-wide systems or records. The appendix lists system notices for common records that are covered by this directive.

System Number	System Name
EEOC/GOVT-1	Equal Employment Opportunity Complaint Records and Appeal Records
FEMA/GOVT-1	National Defense Executive Reserve System
GSA/GOVT-2	Employment Under Commercial Activities Contracts
GSA/GOVT-3	Travel Charge Card Program
GSA/GOVT-4	Contracted Travel Services Programs
MSPB/GOVT-1	Appeal and Case Records
OGE/GOVT-1	Executive Branch Public Financial Disclosure Reports and Other Ethics Program Records (PDF)
OGE/GOVT-2	Confidential Statements of Employment and Financial Interests
	OPM Government-wide Privacy Act Systems
OPM/GOVT-1	General Personnel Records
OPM/GOVT-2	Employee Performance File System Records
OPM/GOVT-3	Adverse Actions and Actions Based on Unacceptable Performance
OPM/GOVT-5	Recruiting, Examining and Placement Records
OPM/GOVT-6	Personnel Research and Test Validation Records
OPM/GOVT-7	Applicant--Race, Sex, National Origin and Disability Status Records

National Archives and Records Administration

NARA 1611
September 18, 2009

SUBJECT: Loans of Archival Holdings to Federal Originators

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Incorporating Change 1, May 13, 2013

Purpose of this transmittal memo. This transmits directive NARA 1611, Loans of Archival Holdings to Federal Originators.

Significant change. A new loan agreement is required (see Appendix A).

~~**Reference to two future directives.** In subparagraph 1611.6j of this directive, there is a reference to two future directives – NARA 1612, Exhibition Loans and Traveling Exhibits, and NARA 1573, Preservation, Security and Transportation Standards for Exhibition of Original NARA Holdings. These two directives are currently under development. NARA 1572 is being revised and its new title will be, 'Preventing the Loss of NARA Holdings.' This new title is referenced in paragraph 1611.4g of the attached.~~

Canceled directives. Parts 2 and 3 of NARA 1701, dated September 1, 1999.
~~Interim Guidance 1611-1, Overdue, Damaged, and Missing Loans of Holdings in NARA's Physical and Legal Custody, is still in effect for other types of loans, but not for this loans directive.~~ This directive now includes its own policy and procedures on overdue, damaged, and missing loans. Interim Guidance 1611-1 was cancelled by Deputy Archivist memo dated January 28, 2013.

ADRIENNE C. THOMAS
Acting Archivist of the United States

Attachment

NARA 1611
September 18, 2009

SUBJECT: Loans of Archival Holdings to Federal Originators

Part 1 - Policy Relating to Loans to all Originators

1611.1 Purpose of this directive

This directive provides policy and procedures for loans of records to the originating Federal executive branch agencies and courts, the Congress, the Supreme Court, and other federal courts from which the records were accessioned or placed in NARA's physical custody. Follow the procedures in the Supplement to this directive when processing a request.

1611.2 Authority for this directive

The Archivist is responsible for the custody, use, and withdrawal of records transferred to the National Archives and Records Administration (NARA) in accordance with 44 U.S.C. 2107 note sec. 3(2), 2108, 2109, 2111 note sec. 101(b)(2), 2112(c), 2118, and 2203(f)(1); E.O. 12667; and 36 CFR 1228.280.

1611.3 Related Directives

a. NARA 1571, Archival Storage Standards;

b. NARA 1572, Preventing the Loss of NARA Holdings;

c. NARA 1573, Preservation, Security and Transportation Requirements for Exhibition of Original NARA Holdings;

d. NARA 1561, Records Emergency Preparedness and Recovery ion NARA Facilities;

e. NARA 1612, Exhibition Loans and Traveling Exhibits; and

f. Interim Guidance 233-1, Food and Drink near Archival and Records Center Holdings.

1611.4 Definition of terms as used in this directive

a. **Borrower** - A Federal executive branch agency or its successor in function or Federal court that requests use of the records it created; a Federal agency that obtains written loan approval from the agency that created the records; the Supreme Court; the Senate and the House of Representatives and their components.

b. **Custodial unit** - A NARA unit responsible for archival holdings, such as:

(1) Archival operations units in Research Services (R); and

(2) Units performing archival functions and holding archival records in other NARA offices.

c. **Holdings** - Records as defined in 44 U.S.C. 3301 that are in both the physical and legal custody of NARA as well as records of the Congress in NARA's physical custody.

d. **Loan** - Temporary removal of holdings from NARA's physical custody to the originator for a purpose other than declassification review or exhibition, or to another Federal agency that obtains written loan approval from the agency that created the records.

e. **Originator** - The Federal entity that created the holdings being requested or maintained them when they were in active use, including a Federal executive branch agency or successor in function [per 44 U.S.C. 290 (14)], federal courts, the Supreme Court, or the Senate and House of Representatives and their components.

f. **Records** – Are defined in 44 U.S.C. 3301 ("includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics") .

g. **Specially protected records** - Holdings determined by managers of custodial units to need protection beyond that normally required for archival records. In making this determination, on the recommendations of knowledgeable archival staff, managers consider whether the holdings are especially vulnerable to theft or likely targets of vandalism. NARA 1572, Preventing the Loss of NARA Holdings, provides guidance on storage and handling of records requiring special protection.

h. **High value holdings** - Holdings determined by the custodial unit to be of significant historic, legal, and/or monetary value. High value holdings may require specific and additional preservation and (or) security measures.

1611.5 What holdings are covered by this directive?

This directive applies to holdings as defined in subpara. 1611.4c.

1611.6 What holdings are not covered by this directive?

This directive does not apply to the following holdings:

a. Records that a Federal agency has transferred to the physical, but not legal custody of NARA, even if the records are scheduled as permanent.

b. Records that the Archivist has authorized a Federal agency to transfer to public or educational institutions or associations in accordance with 44 U.S.C. 2107(3) and 36 CFR 1228.70 – 1228.78.

c. Accessioned electronic holdings.

d. Nixon Presidential historical materials as defined in 44 U.S.C. 2111 note sec. 101(b) (2).

e. Assassination records as defined in 44 U.S.C. 2107 note sec. 3(2).

f. Presidential records as defined in 44 U.S.C. 2201(2) that are in the physical and legal custody of NARA.

g. Classified records, which leave NARA only for declassification review under a Memorandum of Agreement, which defines guidelines, such as handling and special storage requirements and site inspections.

h. Specially protected records.

i. Records being returned in response to a court order.

j. Records that a federal originator is borrowing to use in an exhibit. For guidance relating to borrowing for exhibit purposes see NARA 1612, Exhibition Loans and Traveling Exhibits, and NARA 1573, Preservation, Security and Transportation Standards for Exhibition of Original NARA Holdings.

1611.7 Responsibilities

The following units review and service loan requests for holdings:

a. **The Custodial Unit**

(1) Screens all incoming loan requests for holdings in their custody to confirm that copies will not satisfy the requirement.

(2) Examines the requested records and assesses, if necessary with Preservation Programs (RX), the condition of the requested material. Consult RX when holdings are unstable or are vulnerable to damage due to size or format or if the intended use by the agency may damage or put records in jeopardy.

(3) Authorizes or denies the loan per the decision of the custodial unit head or the director of archival operations, and the signing of the loan agreement by the custodial unit head or the director of archival operations.

(4) Makes loan transportation arrangements, consulting as necessary with the Security Management Division (BX) and RX, and following the policy and procedures in the NARA 1702, Transporting Holdings in NARA's Physical and Legal Custody, to transport holdings to and from originators.

(5) Negotiates a written loan agreement with the borrower per the terms and format in Appendix A, Terms and Conditions for Interagency Loans. If any special conditions exist or special terms are needed, the custodial unit modifies the basic agreement and, as necessary, arranges for a review of the text by NGC. The head of the custodial unit or the director of archival operations signs the agreement for NARA.

(6) Documents and tracks the loan, preferably in a loan database, maintains a dossier of decisions and actions taken, and completes and routes NA Form 14014, National Archives and Records Administration Loan Receipt, following the procedures in the Supplement.

(7) Processes returned loans.

(8) Retrieves overdue loans.

(9) Informs RX, BX, and the Office of the Inspector General (OIG) when a loan is returned with damaged or missing material.

b. **The Security Management Division (BX)**

(1) Advises other NARA offices concerning the security of records considered for loan.

(2) Establishes security measures for NARA records in transit.

(3) Coordinates security arrangements with carriers, at transfer sites, and with federal, state, and local law enforcement.

(4) When a loan is returned with damaged or missing records:

(a) Conducts the Risk Management Review to determine what happened, why it happened, and how, so problems contributing to the loss or damage can be corrected.

(b) Notifies the OIG at the start of the BX Risk Management Review. OIG notification is a separate action from the NAS Risk Management Review.

(c) Coordinates with and notifies NGC, as necessary during the Risk Management review process, as well as other NARA offices that may have a present or future stake in the matter.

(d) When appropriate, notifies federal, state, and local law enforcement and investigative agencies when loaned records are intentionally damaged or stolen and makes sure that actions are being taken to safeguard potential evidence, as well as report, investigate, and recover the missing item.

c. **Preservation Programs (RX)**

(1) On request, reviews the condition of records requested for loan, and recommends, completes or oversees treatment and preservation needs.

(2) Consults with the custodial unit, as requested, and BX about whether to approve or deny a request for original holdings.

(3) Considers with the custodial unit and BX the appropriate method of transportation for the records being loaned, in accordance with NARA 1702.

(4) Examines records that the borrower returns in a damaged condition, determines treatment or housing needs and associated costs, and bills the borrower for costs.

d. **The Executive for Research Services (R) (or his or her designee)**

(1) Arbitrates instances in which the various units cannot agree on whether to loan records.

(2) Considers appeals from originating Federal agencies that have been denied a loan.

(3) Approves extensions of loans beyond 90 days.

(4) On a quarterly basis, reports to the Archivist all loans that are not returned after the overdue notifications and that have not received an authorized extension. (See para.V in the Supplement.)

(5) Consults with NGC regarding actions to recover holdings that are overdue. Works with the custodial unit and NGC to make recommendations to the Archivist for further actions.

e. **The General Counsel (NGC)**

(1) Coordinates, on request, with the custodial unit any special wording needed for the loan agreement to meet unique circumstances relating to the loan.

(2) Works with the custodial unit and R to make recommendations to the Archivist for further actions to recover overdue loans and advises the OIG that holdings are overdue.

1611.8 How are records created by this directive maintained under the NARA records schedule?

a. In custodial units, use file number 1424, Agency Loan Files, and its subparts 1424-1, 1424-2, and 1424-3.

b. In preservation units treating damaged records use file numbers 1435 and 1436.

c. In NGC use file numbers 1103-1a and -b as appropriate.

d. In BX and OIG use file numbers 1208-2a and -b, as appropriate.

Part 2 - Loans to Originating Entities other than the Supreme Court and the Congress

1611.9 What is NARA policy on loans to originators other than the Supreme Court and the Congress?

It is NARA's policy to loan back holdings to requesting agencies only rarely and only for the most compelling reasons as assessed using the factors in para. 1611.10. Whenever possible, NARA offers copies instead of the original documents in NARA holdings. If the records have been reformatted, the originals will not be loaned. The National Archives reserves the right to cancel a loan for good cause at any time, and will make every effort to give reasonable notice thereof. Third party use (i.e., entity other than the original borrower) of records is not permitted.

1611.10 What factors must the custodial unit, in consultation with BX and RX, consider when approving or denying a request for original holdings?

a. Factors that may be the basis for determining that it is appropriate to loan holdings to a requester include:

(1) The requester cannot fulfill their need for the records in any other way.

(2) The requester cannot meet their needs by using the holdings in a NARA facility.

(3) A copy or certified copy cannot be used.

(4) The holdings are in suitable physical condition for transport and use outside of a NARA facility.

(5) The loan is required or authorized by an appropriate statute.

(6) The volume of holdings requested is so large that the custodial unit determines it to be impractical to make and provide copies of the records and the request meets the other applicable criteria in this section.

b. Factors that are the basis for determining that it is not appropriate to loan holdings to a requester include:

(1) The requester has an overdue loan.

(2) The holdings are specially protected records or high value holdings and the Archivist has not approved an exception in writing.

(3) The request is from a Federal agency to enable the agency to answer routine reference inquiries from other agencies or the public.

(4) The holdings are too fragile to be handled or transported safely, or conditions at the requester's facility will endanger the security or preservation of the holdings.

1611.11 Who is authorized to request a loan of original holdings?

Originators must request loans in writing. They include the following:

a. A Federal agency or its successor in function or a federal court can request the holdings it created or maintained when in active use.

b. Federal agencies that obtain written approval from the agency that created the records or its successor may also request a loan. A written copy of the approval must be submitted to NARA with the written loan request.

1611.12 If copies are provided instead of original holdings, what are the costs to the requester?

a. For textual records, NARA provides up to 50 pages per request at no cost to the requester. Beyond that, there is a per-page charge equal to the amount charged in the archival research rooms at the time of the request.

b. For non-textual records, reproduction charges are determined by the current fee schedule costs for the item requested.

1611.13 What is the normal loan period?

The loan period should not exceed 30 calendar days but may be extended if the borrower provides NARA with written justification.

1611.14 Who approves requests for extensions of the loan period?

a. The head of the appropriate custodial unit must approve, in writing, any extension of the loan period. He or she can grant extensions in 30-day increments up to a total of 90 days from the original due date, after ensuring that the conditions that permitted the initial loan continue to prevail.

b. The Executive for Research Services (or his or her designee) must approve extensions for longer than 90 days.

1611.15 Under what conditions may authorized officials deny a loan extension?

Authorizing officials may deny a loan extension if the:

a. Conditions that permitted the initial loan do not continue to prevail.

b. Borrower is found to have damaged the records, mishandled them, or otherwise placed them at risk.

1611.16 When is a loan considered overdue?

A loan is overdue if the borrower does not return the holdings to NARA by the established due date. The borrower must provide a written justification to request extension of the due date, and obtain authorization from the officials in para. 1611.14.

Part 3 - Loans to the Congress and the Supreme Court

1611.17 What is NARA policy on loans to the Congress and the Supreme Court?

NARA may loan records from the Congress and from the Supreme Court back to their originating agencies on a less restrictive basis than holdings from executive branch agencies. This may include waiving the use of the loan agreement format in Appendix A for the records of the Congress. The records of the Congress, including those of United States Senate and the United States House of Representatives, are in NARA's physical custody but not NARA's legal custody. The records of the Supreme Court are in NARA's physical custody but remain in the legal custody of the Supreme Court.

1611.18 Responsibilities in addition to the responsibilities of the custodial units specified in para. 1611.7

a. Holdings of the Congress -

(1) The Director, Center for Legislative Archives (LL), ensures that a loan of U.S. Congress holdings is properly documented.

(2) The Office of the Secretary of the Senate and the Office of the Clerk of the House determines designated individuals authorized to borrow holdings.

b. Holdings of the Supreme Court -

(1) The head of the Archives I reference staff in Archival Operations – Washington, DC (RD-DC), ensures that a loan of Supreme Court holdings is properly documented and returned on the established due date.

(2) The Archives I reference staff in RD-DC maintains a record of Court staff authorized to borrow holdings.

1611.19 Who can request a loan of original holdings?

a. Holdings of the U.S. Senate - NARA normally lends U.S. Senate holdings only to the committee that originated the holdings, a successor committee, or the Secretary of the Senate. Senate Rule XXVI, 10(a), permits access to Senate committee holdings by a senator who is not a member of the committee. In those cases, LL arranges the loan through the Secretary of the Senate and the parent committee.

b. Holdings of the U.S. House of Representatives - Only the designated individuals of the Office of the Clerk of the House of Representatives may borrow House holdings.

c. Holdings of the Supreme Court - Only authorized employees of the Office of the Clerk of the Supreme Court may borrow Supreme Court holdings.

Appendix A - Terms and Conditions for Interagency Loans

Terms and Conditions for Interagency Loans:

NARA is loaning the attached list of holdings of the National Archives (hereinafter holdings) to _____ (hereinafter borrower). Borrower has the authority to enter into the agreement; including the authority to compensate NARA for efforts undertaken, if necessary, to return the holdings to the condition they were when loaned.

Preservation and Use

Each holding is loaned for the benefit of the borrower, and shall be given special care at all times to insure against loss, damage, or preventable deterioration. Precautions must be taken to protect holdings from fire, water, theft, mishandling, dirt and insects, and extremes of light, temperature and humidity while in the Borrower's custody.

The borrower may not mark holdings, attach notes, disband volumes, remove attached records or otherwise alter the format or condition of any record without prior permission from NARA. Eating, drinking and smoking must be prohibited in areas when NARA holdings are stored, used, or otherwise present.

The borrower must receive permission from NARA before photographing, photocopying or scanning holdings and may be required to follow NARA guidelines. The borrower may not place the loaned holdings on display or exhibit unless prior written permission is received from NARA and all guidelines for security and preservation requirements for display have been met.

The borrower must have an up to date emergency plan with a clear chain of command and must maintain current contact information for the borrower's staff and NARA contacts. The borrower must notify NARA if a potential or actual emergency threatens or damages the facility, the area where a NARA holding is stored or reviewed within the facility, the transportation vehicle or route, or the NARA holdings itself.

NARA will review all holdings before shipment; any damage will be noted in a condition report. The borrower must inspect the holdings upon receipt. Unless the borrower gives written notice specifying any additional damage beyond those NARA identified in the condition report, the borrower agrees that it shall be conclusively presumed, as between the borrower and the National Archives, that the borrower has fully inspected and acknowledged that the holding is in the condition indicated on the report created by NARA, and that the borrower is satisfied and has accepted the holdings in such condition. The Archives is to be notified immediately, followed by a full written report, if damage or loss is discovered.

Damage or loss for which the borrower is responsible includes any damage sustained while the holdings are under the control of the borrower, such as: during transport (if the borrower supplied the vehicles and drivers), while in storage on borrower's property prior to use by borrower (i.e. on a loading dock or in a storage facility), and/or while borrower is reviewing the holdings. Exceptions include causes beyond borrower's reasonable control, such as, acts of God, war, riots, civil disturbances, strikes, terrorist acts or credible threat of same.

If conservation treatment is necessary to return holdings to the condition they were in when loaned:

- NARA will determine, based on an analysis of cost and available resources, whether to undertake the treatment in house or through a contract;
- when NARA performs the treatment, the borrower will reimburse NARA for actual costs incurred, including, but not limited to, NARA staff time, equipment use, utility costs, and transportation costs; and
- if NARA contracts for the treatment, the borrower will reimburse NARA for all contract expenses; contractors will be selected by NARA.

Transportation

Transportation of the objects will be handled pursuant to the guidelines in NARA 1702, Transporting Holdings in NARA's Physical and Legal Custody.

Assignment and Transfer

Except for the circumstances outlined in the second paragraph of this section, without prior written consent of the head of the responsible custodial unit, the borrower shall not (a) assign, transfer, pledge, or hypothecate this agreement, the holdings or any part thereof or any interest therein; (b) sublet or lend the holdings or any part thereof, (c) permit the holdings or any part thereof to be used by anyone other than the borrower or the borrower's employees; or (d) permit the holdings to be moved from the location specified within this agreement. The holdings are, and shall at all times remain, the sole property of the Archives, and the borrower shall have no right, title, or interest therein except as expressly set forth in this agreement.

Term of Loan

The term of this loan is _____ days from the date of transfer.

Any extension of the loan period must be approved in writing by NARA. NARA reserves the right to recall the holdings from loan, if necessary. Furthermore, NARA reserves the right to cancel this loan for good cause at any time, and will make every effort to give reasonable notice thereof.

Any specific facility, security, handling or environmental requirements that are a condition of the loan will be specified in an attachment to this loan agreement.

Concurrence:

For the National Archives and Records Administration:

_____ _____

Name and Title Date

For the borrowing Agency:

_____ _____
Name and Title Date

_____
Name of Agency

Attachment: NA Form 14014, National Archives and Records Administration Loan Receipt (this form lists the holdings that are being loaned)

Supplement - Procedures for Loans to Originators

I. REVIEWING AND APPROVING LOAN REQUESTS

Loans to Originating Entities other than the Supreme Court and the Congress

I.1 What does the custodial unit do when a request is submitted?

a. When the originator submits the written request, the custodial unit uses the factors in para. 1611.10 of the Directive, to make a recommendation for approval or denial.

b. The head of the custodial unit or director of archival operations makes the final determination on the request.

I.2 If the request is approved, how does the custodial unit process the loan?

The custodial unit -

a. Negotiates a written loan agreement with the borrower per the terms and format in Appendix A, Terms and Conditions for Interagency Loans.

(1) These terms include the duration of the loan and a commitment by the borrowing agency to pay for conservation treatment on any damaged records.

(2) If any special conditions exist or special terms are needed, the custodial unit modifies the basic agreement and, as necessary, arranges for a review of the text by General Counsel (NGC). The custodial unit head in RD-DC or the director of archival operations in regional archives signs the agreement for NARA.

b. Documents and tracks the loan, preferably in a loan database, maintains a dossier of decisions and actions taken, and completes and routes NA Form 14014, National Archives and Records Administration Loan Receipt, as follows:

(1) Prepares an NA Form 14014 to document the loan and makes sure it is signed by the head of the custodial unit in R or the director of archival operations in regional archives.

(2) Sends the NA Form 14014 to the borrower with the loan.

(3) Ensures that the borrower signs and returns the NA Form 14014 when the loan is received.

(4) Files a copy of the signed loan agreement and the NA Form 14014.

(5) Reviews the 14014 files regularly to anticipate loans that will soon be coming due.

Loans to the Congress and the Supreme Court

I.3 Procedures for processing a loan

a. Whenever possible, the Center for Legislative Archives (LL) or the Archives I reference staff in RD-DC should obtain written permission from the appropriate House or Senate official, or the Office of the Clerk of the Supreme Court (as appropriate) before lending holdings to the Congress or the Supreme Court. This written request may be an e-mail or a letter faxed to the lending custodial unit. When the need for holdings is so urgent that there is no time for a written request before lending the holdings, LL or the Archives I reference staff in RD-DC must obtain a written request within 48 hours after the holdings are loaned.

b. LL or the Archives I reference staff in RD-DC prepares an NA Form 14014 to document the loan.

c. LL or the Archives I reference staff in RD-DC ensures that the borrower signs the NA Form 14014 and files a copy of the form in the appropriate tracking file.

II. DENIAL OF REQUESTS

Loans to Originating Entities other than the Supreme Court and the Congress

II.1 What if a loan request is denied?

If a custodial unit denies a request for a loan, the custodial unit head contacts the requester and:

a. Specifies the reason for the denial;

b. States the conditions under which copies can be provided;

c. Suggests that the requester visit the NARA facility; and

d. Informs the requester of the right to appeal, in writing, to the appropriate office head.

II.2 How can a requester appeal denial of a loan request?

If the custodial unit denies a loan request, the requester can appeal in writing to the Executive for Research Services, National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740-6001.

Loans to the Congress and the Supreme Court

II.3 Does a denial of loans apply?

Since both Congress and the Supreme Court retain legal custody of their holdings deposited with NARA, denial of these requests does not apply.

III. TRANSPORTING LOANS TO THE BORROWER

III.1 What procedures must the custodial unit and the borrower follow to transport NARA holdings to the borrower?

The custodial unit must, in accordance with NARA 1702, Transporting Holdings in NARA's Physical and Legal Custody, and after consultation with RX and BX, determine the appropriate method of transportation, make the necessary arrangements for shipment, and coordinate the movement with the borrower. (See NARA 1702 with regard to shipment, packaging, special transportation arrangements, security, verification requirements, and return arrangements.)

IV. PROCESSING A RETURNED LOAN

Loans to Originating Entities other than the Supreme Court and the Congress

IV.1 What must the custodial unit do to process returned loans?

Immediately upon receipt of the returned holdings, the custodial unit must:

a. Examine the records to ensure that the borrower returned the holdings in the same condition in which they were loaned. (See para. IV.2 for procedures to follow if any holdings are missing or damaged.)

b. Remove the NA Form 14014 from the file, and ensure that the appropriate official (or representative) signs the form to indicate that the holdings have been returned.

c. If the custodial unit uses a tracking database, enter the date that the holdings were returned and any relevant information, such as damage to the records.

IV.2 What if the borrower returns the loan in damaged condition or with holdings missing?

a. If holdings or packaging are found damaged upon return, the custodial unit head:

(1) Immediately documents the nature of damage;

(2) Refers damaged holdings to RX for examination and determination of method of treatment, if necessary (see para. b);

(3) Informs the borrower of any damage believed to have occurred due to their improper handling or negligence and reminds the borrower that they will be responsible for any conservation treatment costs;

(4) Informs the borrower that future loan privileges will be jeopardized unless action is taken to eliminate the risk of damage to the holdings;

(5) Notifies BX; and

(6) Notifies the OIG.

b. RX provides a cost estimate for treatment and RX charges the borrower for services rendered or for the cost of hiring a contract conservator to address any damage due to the borrower's improper handling or negligence.

c. If holdings are missing, the custodial unit must attempt to ascertain the status of missing holdings and notify BX and OIG.

d. The custodial unit head also notifies other units and offices holding records from the same borrowing originator so that they can be aware of the problems in case they also get requests for loans.

Loans to the Congress and the Supreme Court

IV.3 What must the custodial unit do to process returned loans?

Immediately upon receipt of the returned holdings, the custodial unit must:

a. Examine the records to ensure that the borrower returned the holdings in the same condition in which they were loaned.

b. Remove the NA Form 14014 from the file, and ensure that the appropriate official (or representative) signs the form to indicate that the holdings have been returned.

c. If the custodial unit uses a tracking database, enter the date that the holdings were returned and any relevant information, such as damage to the records.

IV.4 What if the borrower returns the loan in damaged condition or with holdings missing?

a. If holdings or packaging are found damaged upon return, the custodial unit head:

(1) Immediately documents the nature of damage;

(2) Refers damaged holdings to RX for examination and determination of method of treatment, if necessary (see para. b); and

(3) Informs the borrower of any damage believed to have occurred due to their improper handling or negligence and works with the borrower, when and if appropriate, to arrange for funds to cover any conservation treatment costs.

b. RX provides a cost estimate for treatment including costs of NARA staff time and supplies or for the cost of hiring a contract conservator to address any damage due to the borrower's improper handling or negligence.

c. If holdings are missing, the custodial unit must attempt to ascertain the status of missing holdings and notify BX and OIG.

d. The custodial unit head also notifies other units and offices holding records from the same borrowing originator so that they can be aware of the problems in case they also get requests for loans.

V. RECOVERING AND REPORTING OVERDUE LOANS

Loans to Originating Entities other than the Supreme Court and the Congress

V.1 What procedures does NARA follow to recover holdings that are overdue?

a. If the loan is overdue, the custodial unit notifies the borrower to either request an extension or promptly return the holdings. Notification by telephone or e-mail is acceptable but the custodial unit must document all actions in writing.

b. If the borrower does not request an extension or does not return the holdings within two weeks of NARA notification that the loan is overdue, the custodial unit head contacts the borrower to determine the reason for delay.

c. If the custodial unit does not receive the extension request or the holdings within two weeks after the second contact, the custodial unit head creates a dossier containing a memorandum explaining the circumstances, a copy of the loan agreement, NA Form 14014, a written summary of any verbal contacts, copies of all relevant correspondence and e-mail exchanges, and any other pertinent documentation.

d. R custodial units send the dossier to R through the appropriate access coordinator.

e. R immediately consults with NGC, who in turn advises the OIG that holdings are overdue.

f. R, working with the custodial unit and NGC, make recommendations to the Archivist for further action.

g. The custodial unit head also notifies other units and offices holding records from the same borrowing originator so that they can be aware of the problems in case they also get requests for loans.

V.2 Reporting overdue loans to the Archivist

On a quarterly basis, R must report to the Archivist all loans that have not been returned after the overdue notifications and that have not received an authorized extension. R must submit this report within 30 calendar days after the end of each fiscal quarter and should include:

a. Borrower's name;

b. Description of holdings;

c. Record group number or collection;

d. Quantity of holdings (boxes, cubic feet, etc);

e. Loan date;

f. Due date (last date, including any extensions, that the loan was to be returned to NARA); and

g. A narrative and documentation of steps that the custodial unit has taken to recover the loan.

Loans to the Congress and the Supreme Court

V.3 Tracking or reporting overdue loans

a. The Archives I reference staff in RD-DC contacts the Office of the Clerk of the Supreme Court to verify that the loan needs to be extended.

b. For holdings that have been on loan for more than 30 days, the Archives I reference staff in RD-DC contacts the Clerk of the Supreme Court about any holdings that have not been returned.

c. For the quarterly report to the Archivist, Archives I reference staff in RD-DC provides to R a list of loans that are overdue for more than three months. Include the loan number, record group, date of the loan, the organization (committee) or person (Secretary or Clerk) who borrowed the holdings, and the due date.

d. LL does not place a time limit on loans to Congress.

National Archives and Records Administration

Transmittal Memo

DATE: September 30, 2015

TO: All Staff

SUBJECT: NARA 1653, NARA RECORDS REPRODUCTION FEE SCHEDULE

Purpose: This directive establishes the fees to be charged by NARA to the public for reproductions of records. This directive also provides internal NARA policies and procedures for amending and implementing the NARA records reproduction fee schedule. The fee schedules are the appendices A and B and list all of the authorized reproduction fees that may be charged to the public or other Federal agencies.

Background/Significant changes: This directive removes the language allowing for *Bill Me* orders. It also incorporates information relating to NARA's new electronic transfer system for records reproductions.

Available forms: This directive and its attachments provide guidance on the use of forms numbered NATF 81 through NATF 86 and NATF 90 through NATF 93.

Canceled forms: None.

Canceled policies: NARA 1653, NARA Reproduction Fee Schedule, dated May 11, 2015.

Related policy:

- NARA 1602, Access to Records Requested under the Freedom of Information Act.
- NARA 1653-3, Digital Fees for Presidential Libraries.
- NARA 1653-11, NARA Fees for Reproductions of Court Martial Records Held by the National Archives at St. Louis.
- NARA 1653-14, NARA Fees for Printing from Public Access Personal Computers (PAPCs).

Effective date: This policy is effective November 6, 2015.

National Archives and Records Administration

Contact information: You may direct questions about this policy to Peter Staub, Trust Fund Division, in room 5100, AII; by telephone on 301-837-2963; or by e-mail.

DAVID S. FERRIERO
Archivist of the United States

Attachments

SUBJECT: NARA RECORDS REPRODUCTION FEE SCHEDULE

1653.1 Policy.

a. NARA charges fees to recover all of its costs for providing records reproduction services to the public.

b. If a product does not appear in Appendices A or B, indicating approval of the Archivist, you may not charge a fee for the service, with exceptions noted below. Paras. 14 and 15 of the Supplement to this directive specify what you must do to add an authorized fee.

c. Additional policies may be issued at anytime, authorizing fees during a pilot project fee study.

d. After NARA provides a digitized copy of a record to a requestor who has paid the assessed fee, we may create and retain an additional copy of that digitized record for our own use (i.e., post a copy on-line (for free access), re-package a copy of the record in another records reproduction product, or use that copy as a "preservation" or "reference" copy, etc.).

(1) The fees assessed and paid by the requestor for the first copy of a record are set to recover the cost of that copy.

(2) If subsequent researchers request a copy of the same record, they may be made aware of the existence of a free copy available on-line. However, if the staff member fulfilling the request is not aware of the existence of a free copy, the staff member may make or order a new reproduction and assess a fee to the subsequent researcher, allowing NARA to recover the cost of producing a record reproduction.

e Record reproductions should be made from preservation copies or reformatted surrogates when they exist.

1653.2 Coverage.

a. In addition to records reproduction orders, the fee schedule also applies to archival records requested under the Freedom of Information Act (FOIA). It does not apply to NARA's operational records, including NARA finding aids.

b. This fee schedule applies to all NARA custodial units that provide records reproductions, with the exception of Presidential Libraries, each of which maintains a separate fee schedule.

NW: 15596 DocId: 70098830 Page 3

1653.3 Responsibilities.

a. The Archivist of the United States approves the NARA fee schedule and all changes to it.

b. The National Archives Trust Fund Division (BCT):

(1) Conducts periodic cost analyses of the NARA fee schedule to determine if fees should be changed;

(2) Recommends changes to existing fees;

(3) Reviews requests for new reproduction products;

(4) Recommends fees for new reproduction products; and

(5) Advises Agency Services (A), Research Services (R), and Legislative Archives, Presidential Libraries, and Museum Services (L) on changes to fees.

c. Program offices:

(1) Ensure that correct fees are charged;

(2) Fulfill customer orders and apply fee schedule; and

(3) Propose new products to be added.

1653.4 Definitions.

a. **Archival records.** Records that have been accessioned into the legal custody of NARA, donated historical materials in the legal custody of NARA and its Presidential libraries, and Congressional, Supreme Court, and other historical materials in NARA's physical custody and for which NARA has a formal agreement for their permanent retention.

b. **Operational records.** Records that NARA creates or receives in carrying out its mission and responsibilities as an Executive branch agency. Includes NARA-produced finding aids except tape logs prepared in processing Nixon Presidential materials and the database and related finding aids to the John F. Kennedy Assassination Records Collection.

c. **Publication.**

NW: 15596 DocId: 70098830 Page 4

(1) Any printed or digital works extracted from NARA Holdings and offered for sale or distribution as a single unit.

(2) Taking multiple original documents and combining them into a set, periodical, book, etc.

(3) A set of records or documents purposefully grouped by subject matter for sale to the public.

(4) A single unit descriptor created to facilitate a more effective and efficient reproduction process (i.e., fixed-fee product creation for sale over NARA's online ordering system).

(5) A set of records that is grouped and stored in a series on microfiche, microfilm or a dataset and indexed at the media unit level. (i.e., roll, sheet, dataset; ex, DN1924, Records of the Foreign Exchange Depository Group of the Office of the Finance Adviser, OMGUS, 1944-1950 [RG 260]).

d. **Product.**

(1) Commercial merchandise purchased or commissioned for the purpose of resale via eCommerce or over-the-counter.

(2) Mass- or multiple-produced goods.

(3) A reproduction or publication where value has been added (i.e., grouping of two like reproductions into one (photo and .mp3 of Adlai Stevenson), digitizing and adding metadata to documents that were previously hardcopy).

e. **Records center records.** Federal records in the physical custody of NARA records centers, but legal custody remains with the agencies that created them.

f. **Reproduction.**

(1) The duplication of an original document, video, audio, photograph, etc. from NARA holdings.

(2) The resultant facsimile of a document, photo, etc. being placed on a photocopier/scanner and copied, either via self-service or by NARA.

(3) The duplication of a single (or multiple) data file(s).

(4) Copying a single page or multiple pages from a publication.

(5) Copying a single file or multiple files from a larger data set.

NW: 15596 DocId: 70098830 Page 5

g. **Records reproduction fee.** The price researchers pay for paper, microfilm, microfiche, or digital copies of archival records. Certification of archival records is also a records reproduction fee, as defined in 36 CFR § 1258.

h. **Records reproduction order.** Researcher request for copies of specific archival or records center records made in a specific format, including certification of same.

1653.5 Authorities.

a. 44 U.S.C. § 2116(c) authorizes NARA to charge a fee for making or authenticating copies or reproductions of materials transferred to the Archivist's custody.

b. 44 U.S.C. § 2307 authorizes the Archivist of the United States, as Chairman of the National Archives Trust Fund Board, to use the trust funds to prepare and publish special works and collections of sources; prepare, duplicate, edit, and release historical photographic materials and sound recordings; and sell those publications and releases at a price that will cover their cost, plus ten percent.

c. 36 CFR 1258 describes the allowable costs which make up NARA's records reproductions fees, how NARA calculates these fees, how NARA develops and publicizes new records reproductions fees, and NARA's payment and refund policies.

d. OMB Circular A-130, Management of Federal Information Resources, indicates that fees may be assessed to the direct recipient of a benefit even though all or part of the benefit may then be passed to others at no cost. NARA does not have to allocate costs to the public if the public's benefit is incidental (not independent) to the benefit of the individual, but may recover the full cost of the benefit from the individual. This circular further indicates NARA's obligation to avoid establishing restrictions or charging fees on the reuse, resale or re-dissemination of Federal dissemination products.

e. NARA 101, NARA Organization and Delegation of Authority, authorizes the National Archives Trust Fund Division (BCT) to review and approve requests for new fees and changes to existing fees.

f. Archives 1400, Chapter 7, Reference Service, Part 3, Use of Records, restricts the use of original records when microfilm or other copies are available.

1653.6 Releasability.

Limited. This directive is approved for public release with the exception of Appendix B.

1653.7 Records Management.

a. NARA Records Reproduction Fee Schedule (e.g., cost analyses, revisions to existing fees, and additions of new products and fees):

(1) BCT uses file numbers 214-1 and 214-2 ("NARA Fee Schedule Files");

(2) Research Services, the National Personnel Records Center (AFN), and Presidential Libraries use file numbers 214-2 and 214-3; and

(3) Field sites (except for AFN) use file number 1343-2, "Records Center Services: Reference/Records Services/Internal Operations."

b. Reproductions of Holdings in Washington, DC and College Park, MD:

(1) Research/Agency Services – When fulfilling customers' orders, follow instructions for the data/series, as applicable:

(a) File number 1807-1 ("SOFA" System: "Customer profile data");

(b) File numbers 1807-2a, b, and c ("SOFA" System: "Order transaction files" [NATF Form 72 quotes, orders, and canceled orders]);

(c) File number 1807-3 ("SOFA" System: "Fulfillment-related records…" [e.g., NATF Form 80 Series]);

(d) File numbers 1421-2 ("Routine [reference] inquiries…") or 1421-3 ("[Reference] correspondence…relating to: significant persons, subjects, or events; noted researchers…; or replies involving repetitive, difficult, or complex research"); and

(e) File number 1423-2 ("Reproduction Service Files: Reproduction requests…and related records") – Use only for transactions from walk-in customers ("cash and carry" payments to BCT cashiers).

(2) BCT– When processing customers' payments, follow instructions, as applicable, for:

(a) File number 1805-1 ("Order Fulfillment and Accounting System [OFAS] and Related Records: Order history file"); and

(b) File numbers 1805-2 a or b ("OFAS: Order transaction files" [Unpaid/Paid BILL ME orders, credit card orders, and all other transaction records]).

c. Reproductions of Agency Services Holdings (EXCLUDES National Personnel Records Center in St. Louis, MO):

(1) Use file number 1474-3a, "Archives Services: Reference…," when responding to and fulfilling reproduction requests that are received via mail, e-mail, fax, or transcribed telephone call.

(2) Refer to file number 267-1, "Collections and Expenditures of Funds…," when:

(a) Fulfilling customers' online orders (received via NARA's online ordering system/SOFA); and

(b) Using Point-of-Sale (POS)/OFAS to process customers' payments that are received via mail, fax, or online ordering system/SOFA, or as POS transactions (walk-in customers only).

(3) See file number 1343-2 for records relating to scanning projects that are undertaken with companies or organizations.

d. Reproductions of Military Personnel Records (e.g., Official Military Personnel Files) (see Part VI of this directive) and Military/Medical Records:

(1) When responding to and fulfilling requests for copies of military personnel records and military/medical records:

(a) Use file number 1340-1, "Case Management and Reporting System (CMRS) and Registry Files: Customer requests ("Scanned paper") – SF 180s, forms, and letters…"; and

(b) Follow instructions for file numbers 1340-2a, "CMRS and Registry Files: CMRS Data…," and 1340-2b, "CMRS…Output: Access Information ("Disclosure Data Extract").

(2) When processing customers' payments (in POS/OFAS), follow instructions, as applicable, for file numbers 1805-1 and 1805-2a or 1805-2b.

(3) When making reproductions for walk-in customers – Use file number 1420-1 or 1420-2 ("Research Room Reference Service Files: Copies of reference service slips (pink copies) and Duplicate copies of reference service slips (white copies)).

e. Reproductions of Civilian Personnel Records (e.g., Official Personnel Folders) (see Part VI of this directive):

(1) When responding to and fulfilling reproduction requests that are received via mail or fax – Use file number 1421-2 or 1421-3.

(2) When making reproductions for walk-in customers – Use file number 1420-1 or 1420-2 ("Research Room Reference Service Files: copies of reference service slips (pink copies) and duplicate copies of reference service slips (white copies))."

(3) When processing customers' payments (in POS/OFAS), follow instructions, as applicable, for file numbers 1805-1 and 1805-2a or 1805-2b.

f. Reproductions of Presidential Library Holdings:

(1) When responding to and fulfilling reproduction requests received:

(a) Via mail, e-mail, fax, or transcribed telephone call – Use file numbers 1421-1 ("Reference Service Communication Files:...registers and logs…") and 1421-2 or 1421-3; and

(b) From on-site researchers – Maintain records in the "Researcher Case Files" (file number 1470-1 or 1470-2).

(2) When processing customers' payments, follow these instructions:

(a) Maintain memorandum copies of documents for administration of libraries' Trust Fund reproduction services programs, including data about collection of Trust Fund payments and recognition of revenue and liabilities. Keep these documents in a "Financial Transactions File" that should include: receipts, bills, vouchers, coding documents, purchase orders, batch sheets, deposit tickets, invoices, and related records. NARA's financial services bureau (Bureau of the Public Debt [BPD] since October 2005) maintains the auditable copies of these records.

(b) For "Detail [financial] records" (cash receipts journal, transaction registers, and related records) – Cut off annually (i.e., end of fiscal year) and destroy 2 years from cutoff date.

(c) For "Summary [financial] records" (records used as source documents for entry into BCT's accounting system and related records) – Cut off annually (i.e., end of fiscal year) and destroy 2 years from cutoff date.

(d) For "Records documenting refunds of monies to customers" – Cut off annually (i.e., end of fiscal year) and destroy 2 years from cutoff date.

SUBJECT: NARA RECORDS REPRODUCTIONS FEE SCHEDULE PROCEDURES

Part I – Information about Records Reproduction Fees

1. Must reproduction orders be prepaid?

Yes, all reproduction orders must be prepaid.

2. May I charge a lower or higher fee in special circumstances?

Because the fees are set to recover NARA's costs on a nationwide basis, you may not reduce or raise a fee without specific authorization from BCT for an individual order (see 36 CFR § 1258).

3. What forms of payment are acceptable for reproduction orders?

As provided in 36 CFR § 1258, fees may be paid in cash, or by check, money order, or select credit cards. However, some NARA facilities are discontinuing, or have discontinued, the acceptance of cash, check, and/or money order.

4. How do I account for free reproductions?

If you are providing a free reproduction that meets one of the special circumstances in 36 CFR §1258, the cost of the reproduction is charged to your unit's OE or revolving fund account.

5. How do I charge for shipping?

a. Shipping is normally handled by USPS and the cost for this service is already incorporated into the established reproduction fee.

b. If a customer requests that the order be sent using an expedited service (e.g., FedEx or UPS), use the customer's account number on the air bill. If the customer does not have an account number, use the NARA account and charge the current expedited shipping fee of $30.00.

c. If a customer requests that the order be sent via an international expedited service (e.g., FedEx or UPS), you must use the customer's account number on the air bill. NARA employees should not ship expedited international customer orders using NARA account numbers.

d. In the case of reproductions shipped via UPS: **UPS will not deliver to a P.O. Box. A street address is needed in these cases.**

6. Why do we impose a minimum order charge and what is the fee?

The minimum order charge is imposed to recover NARA's cost to process and send small orders. The current minimum order fee is $20.00 per order, even if the order is sent electronically.

7. When does the minimum order apply?

The minimum order applies to all orders under $20.00, except for Draft Cards and Naturalization Records. To determine if the minimum order fee applies, calculate the total cost of the record reproductions. If the total cost **is less than or equal to** $20.00, charge the $20.00 minimum order fee (aside from a few exceptions - see examples below). The cost of record certification is *not* included when determining whether the minimum order fee applies.

a. **Example 1:** The customer orders a copy of a 15-page document. The cost of the copies is $12.00. Because the total ($12.00) is less than the minimum order fee of $20.00, the minimum order fee applies and the customer is charged $20.00.

b. **Example 2:** If the customer orders a copy of a ten-page document and asks to have it certified and mailed, the customer would be charged $35.00 [minimum order charge (25 pages or less) added to the cost of the certification at $15.00]. The customer is charged the minimum order charge; certifications are *not* included when determining whether the minimum order fee applies.

c. **Example 3:** If the customer orders a certified Naturalization Record, the customer would be charged $25.00 (cost of the Naturalization record at $10.00 added to the cost of the record certification at $15.00). The customer is NOT charged the minimum order charge. Accessioned Draft Registration Cards and Naturalization Records are not subject to the minimum order.

d. **Example 4**: The customer orders a copy of a 26-page document. The cost of the copies is $20.80. The order total is greater than the minimum order. The customer is NOT charged the minimum order charge.

e. **Example 5:** The customer orders two accessioned draft cards. The cost of the copies is $14.00. The order total is under $20.00; however, accessioned draft cards and accessioned naturalization records are exempt from the minimum order. The customer is NOT charged the minimum order charge.

f. **Example 6:** The customer orders a copy of a 25-page document. The cost of the copies is $20.00. The order total is equal to the minimum order. The minimum order is used in this case, not the per page copy charge.

g. **Example 7:** The customer orders an accessioned draft card plus four reproductions of other records. [i.e., $7.00 for the Draft Registration Card, plus the per page rate (80¢ up to the $20.00 minimum order charge)]. The order is subject to the minimum order charge.

8. When are "rush" orders and "rush" fees authorized?

NW: 15596 DocId: 70098830 Page 11

Rush orders are handled on a case-by-case basis. Staff may be able to accommodate a rush order but this cannot be guaranteed. No extra charges apply for *processing* a rush order, a $30.00, per order, charge applies for expedited shipping.

9. What is BCT's return policy?

Due to the age, original media type and general condition of many of the items in NARA's holdings, it is occasionally difficult to make a legible reproduction. Archivists are trained to notify customers if they anticipate that the original will result in a reproduction of questionable legibility prior to proceeding with the reproduction process. They will only proceed with the approval of the customer. After a record reproduction is completed, the product is reviewed to determine if it is an accurate representation of the original item. Because of this, NARA does not provide refunds except in special cases. If a customer requests a refund, a review is made of the order to determine if the customer was properly notified of the questionable nature of the original and if the product is a true representation of the original. If the customer authorized proceeding and the product is a true representation of the original, no refund will be issued.

10. How do I charge for orders in progress when new fees are made effective?

Use the following chart to determine which fee to charge. If you have questions about a specific order, contact BCT by phone or e-mail.

If the order . . .	Charge the fees in the . . .
was received by the NARA unit before Nov 6, 2015	May 11, 2015 fee schedule
was received by the NARA unit on or after, Nov 6, 2015	,Nov 6, 2015 fee schedule

11. How do I charge for certifications and NARA seal embossing?

Certifications will be charged per 150 pages certified; NARA seal embossing are charged per impression. Certifications and NARA seal impressions are add-on services, the cost of which is not used to determine minimum reproduction order fees. See some examples below:

a. **Example 1:** The customer orders a 225 page certified bankruptcy case file. The cost of the copies is $90.00 for the first 150 pages, then the customer is charged $22.00 per 15-minutes of work (the $22.00 per 15-minute labor rate applies only to Federal Records Centers). In addition, the customer is charged $30.00 for certifications ($15.00 for the certification of the first 150 pages and $15.00 for the remaining 75 pages).

b. **Example 2:** The customer orders a 130 page certified bankruptcy case file. The cost of the copies is $90.00. Since the total page count is 150 or less, the cost of a single certification is $15.00. The customer is charged $105.00

c. **Example 3:** The customer orders a certified Naturalization Record; the customer would be charged $25.00 (cost of the Naturalization record at $10.00 added to the cost of the record certification at $15.00). The customer is NOT charged the minimum order charge. Accessioned Draft Registration Cards and Naturalization Records are not subject to the minimum order.

d. **Example 4:** The customer orders a copy of a ten-page document and asks to have it certified and mailed; the customer is charged $35.00 [minimum order charge (25 pages or less) added to the cost of the certification at $15.00]. The customer is charged the minimum order charge; certifications are *not* included when determining whether the minimum order fee applies.

e. **Example 5:** The customer orders a 26-page NARA seal impressed archival reproduction. The customer wants the first page impressed. The cost of the copies is $20.80. The cost of a single NARA seal impressed $2.50. The customer is charged $23.30.

f. **Example 6:** A walk-in customer makes one (1) reproduction on a NARA-owned self-service machine. That customer then approaches research room staff for a seal impression. The customer is charged $2.50.

g. **Example 7:** The customer orders a copy of a ten-page (10) document and asks to have it impressed and mailed, the customer would be charged $22.50 (minimum order charge of $20 (20 pages or less) added to the cost of the impression at $2.50). The customer is charged the minimum order charge; NARA seal embossments are not included when determining whether the minimum order fee applies.

12. Where can I get a paper seal embosser with the NARA seal?

There are a number of sites that sell paper seal embosser. Below is a short list:

a. http://www.customembossers.com/iconlogodesk.shtml

b. http://www.bizsiteusa.com/seals.html

c. http://www.thestampmaker.com/departments/embossers-and-seals.aspx

d. http://www.abc-i.com/check_document_stampers/manual_embossers.htm

BCT will provide the NARA seal artwork as a high-resolution file. Offices should not create their own.

13. How should the NARA seal be embossed on reproductions?

a. The National Personnel Records Center and the National Archives at St. Louis usually apply the seal to the bottom right corner of reproductions. Embossments should

be done in the corner where the seal will have the least impact on significant data from the reproduction.

b. Normally, only the first sheet of each reproduction order is embossed. For example, if a customer has a ten-page document and requests an embossment, apply the seal only to the first page. If the customer requests that the seal be applied to multiple documents, the seal fee is charged for every document that is embossed.

Part II - Requesting Fees for New Reproduction Products

14. How do I determine the fee for a product that is not listed?

If you are not sure whether the product being requested is covered by the authorized fees, contact BCT for clarification. BCT will provide the correct product code or will instruct you on how to propose a new product.

15. How do I propose a new product to be added?

a. Prepare a justification for your proposed product that includes, at a minimum, the following information:

(1) Estimated monthly volume of orders at your location;

(2) Identification of the equipment and supplies required to make the product and also the estimated cost of the equipment (if it must be acquired) and supplies;

(3) Identification of any products that will be replaced by the proposed product;

(4) Identification of other NARA units that may have a demand for the proposed product; and

(5) Any other information that will help BCT to analyze your proposal.

b. Send the justification to your office head, through appropriate channels, for concurrence and forwarding to BCT.

16. How does BCT evaluate a proposal for a new product?

a. BCT assesses the potential customer base for the proposed product, consulting other NARA offices.

b. If the potential demand warrants, BCT prepares a cost analysis and develops a proposed recommended fee for review by the Chief Financial Officer (BC) and approval by the Archivist.

NW: 15596 DocId: 70098830 Page 14

c. If approved, BCT prepares a change to the fee schedule and generates an interim guidance, where the new fee will remain for at least one-year.

Part III - Fees for Non-digitized Audiovisual Reproduction

17. How do I calculate fees for audiovisual reproductions?

The fee for an audiovisual reproduction is calculated by adding the actual vendor charge for the reproductions and the archival handling fee for each item pulled for reproduction. If a customer orders multiple copies made from a single original in one order, the archival handling fee is charged only on the initial copy. The fees are submitted to the vendor who reimburses NARA for the archival handling of the records.

a. **Example 1:** At an archival facility in the field, a customer requests a copy of each of three different photographs. The customer is charged $24.75 (3 times the archival handling fee of $8.25) plus the actual vendor charges for the specific copies.

b. **Example 2:** At the same archival facility, another customer requests that three copies of a single photograph be made. That customer is charged $8.25 plus the actual vendor charges for the copies.

Part IV - Fixed-Fee Orders

18. How can customers place fixed-fee orders?

a. Fixed-fees include the following:

(1) NATF Form 81, Order for Copies of Ship Passenger Arrival Records

(2) NATF Form 82, Order for Copies of Federal Census Records

(3) NATF Form 83, Order for Copies of Eastern Cherokee Applications

(4) NATF Form 84, Order for Copies of Land Entry Files

(5) NATF Form 85, Order for Copies of Military Pension or Bounty Land Warrant Applications

(6) NATF Form 86, Order for Copies of Military Service Records (pre-20th Century)

(7) World War I Era Accessioned Draft Cards

(8) Accessioned Naturalization Records

(9) NATF Form 90, Order for Copies of Bankruptcy Cases

NW: 15596 DocId: 70098830 Page 15

(10) NATF Form 91, Order for Copies of Civil Cases

(11) NATF Form 92, Order for Copies of Criminal Cases

(12) NATF Form 93, Order for Copies of Court of Appeals Cases

b. Customers can access the online ordering system web site to place a fixed-fee order. The customer can also access the online ordering system web site through a link on www.archives.gov.

c. Customers may request paper copies of NATF Form 80s via phone (1-866-272-6272), fax (301-837-0483), online (see the web page entitled "Contact Us" on www.archives.gov.) and postal mail. The mailing address is:

National Archives and Records Administration (RD)
8601 Adelphi Road
College Park, MD 20740-6001

d. Customers may obtain printable copies of NATF Forms 90 on the web at http://www.archives.gov/research/court-records/bankruptcy.html.

e. Completed forms should be sent to the addresses listed on the forms (it is noted that customers should be encouraged to use the online ordering system whenever possible).

19. What if customers use superseded NATF forms to place fixed-fee orders?

We cannot accept orders on paper forms that reflect a superseded fee schedule because we are obligated to recover the full cost of the reproductions. BCT makes every effort to ensure that current forms are available for distribution on and after the effective date of any fee schedule revision. If the Archives receives superseded forms from customers on or after the issuance of a revised fee schedule, they return the forms to the sender with an explanation of the new fee schedule and forms that are now in effect and send copies of the new forms.

Part V - National Archives at St. Louis Reproductions

20. How can customers place orders for fixed-fee Archival Official Military Personnel Files (OMPFs)?

a. The OMPFs listed below are in the legal custody of the National Archives at St. Louis (RL). Much of the written reference work on these records is processed through the staff of the National Personnel Records Center (AFN) which has the physical custody of OMPFs that are not yet accessioned.

b. An OMPF is accessioned 62 years after the veteran is separated from service through discharge, retirement, or death in service. The following is a list of accessioned OMPFs with the earliest dates contained in each series.

(1) U.S. Navy Enlisted OMPFs with discharge dates beginning in 1885;

(2) U.S. Navy Officer OMPFs with discharge dates beginning in 1902;

(3) U.S. Marine Corps Enlisted OMPFs with discharge dates beginning in 1906;

(4) U.S. Marine Corps Officer OMPFs with discharge dates beginning in 1905;

(5) U.S. Army OMPFs with discharge dates beginning in 1912;

(6) U.S. Coast Guard OMPFs with discharge dates beginning in 1885; and

(7) U.S. Air Force OMPFs with discharge dates beginning in September 1947.

c. To order a record, customers may:

(1) Create a web request at http://vetrecs.archives.gov (veterans and next of kin ONLY).

(2) Fax a request to AFN at 314-801-9195.

(3) Send a written request to:

National Personnel Records Center
1 Archives Drive
St. Louis, MO 63138-1002

(4) The Standard Form 180, Request Pertaining to Military Records, is often used to request copies of archival military records. See http://www.archives.gov/research/order/standard-form-180.pdf.

(5) Visit the National Archives at St. Louis research room. To make an appointment, customers may call 314-801-0850 or send an email to stlarr.archives@nara.gov.

21. How can customers place orders for fixed-fee Archival Official Personnel Folders (OPFs)?

To order records, customers may:

a. Fax a request to RL at 314-801-9187

b. Send a written request to RL at

National Archives at St. Louis
P.O. Box 38757
St. Louis, MO 63138

c. Visit the National Archives at St. Louis research room. To make an appointment, customers may call 314-801-0850 or send an email to stlarr.archives@nara.gov.

22. How can customers place orders for Digital Reproductions of Persons of Exceptional Prominence (PEP) Folders?

a. PEP records are the subset of OMPFs that pertain to veterans who are well-known to the public. Some of the PEP records are available only in paper form, while others have been digitized and are sold in DVD format. The list of PEP records on NARA's website, http://www.archives.gov/st-louis/military-personnel/public/persons-of-prominence.html, shows which PEP records are available in digital format (along with the associated costs).

b. To order a PEP record that is not available in digital format, customers may follow the procedures in Question 20 above.

c. To order a digital PEP record, customers may:

(1) Fax a request to RL at 314-801-9187.

(2) Send a written request to RL at

National Archives at St. Louis
P.O. Box 38757
St. Louis, MO 63138

(3) Visit the National Archives at St. Louis research room. To make an appointment, customers may call 314-801-0850 or send an email to stlarr.archives@nara.gov.

Part VI - Digitized/Digital Reproductions

23. What are the scan type definitions and equipment specifications for digitized reproductions?

BCT provides digitized reproductions in three categories: self-service scanning, basic digitized scans, and NARA enhanced scans. Below are definitions and specifications for each type of reproduction.

a. **Self-Service Scanning** – The specifications for self-service scanning are for digitized scans made by customers who are visiting a NARA operated research room and using NARA owned equipment. Reproduction scans will adhere to the following specifications:

- Minimum Scanner Resolution: 300 ppi @ original document size. Customers may have the option to lower the scanner resolution.
- Scanner Bit-Depth: 1 bit for Black-and-White, 8 bits for grayscale, and 24 bit for color.
- Color Options: Black-and-White, Grayscale, Color.
- Minimum Document Scan Size: 8 ½" x 14". Scan size will vary by location.
- Image Adjustments: Customers will be limited to image adjustments available in the scanner driver (generally brightness and contrast).
- Possible File Types: .TIF, .JPG, .BMP, .PDF. Available file types may vary by locations.

b. **Basic Digitized Scan and Digitized Reproductions of Film Negatives** – The basic digitized scan will be used for the vast majority of NARA-made digitized reproductions; digitized reproductions of film negatives will follow the same scan specifications as the basic digitized scan. This type of reproduction can be used for textual, cartographic, and photographic reproductions. This product is equivalent to the Digitization Services Branch (VIS) Distribution Image (IMG-D6) as described at http://www.archives.gov/preservation/products/definitions/copy-types.html. Reproduction scans will adhere to the following specifications:

- Minimum Scanner Resolution: 300 ppi @ original document size or 3000 pixels on the long dimension for film scans (negatives will be inverted to a positive tonal orientation). Customers may request lower scanner resolutions.
- Maximum Scanner Resolution: 400 ppi @ original document size or 4000 pixels on the long dimension for film scans (negatives will be inverted to a positive tonal orientation).
- Scanner Bit-Depth: 1 bit for Black-and-White, 8 bits for grayscale, and 24 bit for color.
- Color Options: Black-and-White, Grayscale, Color.
- Minimum Document Scan Size: 8 ½" x 14". Scan size will vary by location.
- Image Adjustment: NARA technicians will make **no** adjustments to the scanned image.
- Possible File Types: .TIF, .JPG, .BMP, .PDF. Available file types may vary by locations.

c. **NARA Enhanced Scan** – The NARA Enhanced scan will be only available at locations capable of meeting the capabilities discussed below. This type of reproduction can be used for textual, cartographic, and photographic reproductions. This product is equivalent to the Digitization Services Branch (VIS) Standard Distribution Image (IMG-

D1) as described at http://www.archives.gov/preservation/products/definitions/copy-types.html. Reproduction scans will adhere to the following specifications:

- Minimum Scanner Resolution: 400 ppi @ original document size or 4000 pixels on the long dimension for film scans (negatives will be inverted to a positive tonal orientation).
- Minimum Scanner Bit-Depth: 1 bit for Black-and-White, 8 bits for grayscale, and 24 bit for color.
- Color Options: Black-and-White, Grayscale, Color.
- Minimum Document Scan Size: 8 ½" x 14". Scan size will vary by location.
- Image Adjustment: Color and tone reproduction has been adjusted for generic monitor display. System calibration and/or image processing has been performed to ensure a Federal Agency Digitization Guideline Initiative (FADGI) image quality rating of at least 1-star in all categories (http://www.digitizationguidelines.gov/still-image/).
- Possible File Types: .TIF, .JPG, .BMP, .PDF. Available file types may vary by locations.

24. How can I determine if I have the appropriate equipment to make digitized reproductions?

Hardware determinations may be assisted by consulting the Digitization Services Branch (VIS). Additional information may also be found here: http://www.archives.gov/preservation/products/definitions/copy-types.html. Any business unit unable to meet the hardware determinations must not offer digitized reproductions. Further, NARA Enhanced scans should only be offered by those who can meet the FADGI 1-star ratings in all categories.

25. How are digitized reproductions delivered to the customer?

Images are burned onto CD or DVD, uploaded to NARA's electronic transfer site, or sent via email.

a. If file size permits and the customer order specifies, images can be sent via e-mail. Image size for email is limited to 5 MB (megabyte). The staff member sending the e-mail should place a read receipt on outgoing emails. This option is not available via the online ordering system, aside from WWI era Draft Registration Cards.

b. If the customer requests to have their reproduction delivered via electronic transfer, the staff member uploads the file(s). The customer is then notified electronically and automatically that the file is available. The customer must have provided a valid email address to use this option.

b. A customer may request that a digitized reproduction be sent on CD/DVD via UPS or USPS, depending upon type of reproduction. If a CD will not hold all digitized images, a DVD may be used, if the office performing the reproductions has the capability. If DVD is not an option, multiple CDs may be used. When providing the customer with multiple discs, the same medium should be used (i.e., a customer should never receive one DVD and one CD).

(1) A CD holds approximately 660 MB of information.

(2) A DVD holds approximately 4.7 GB of information.

26. Is a fee to be charged for the digitized media used (i.e., CD/DVD)?

No; the cost for the CD/DVD is included in the price of a reproduction. NARA will assess a fee of $2.00 to a researcher requesting a blank CD/DVD for use in self-service digital reproductions, at NARA locations that choose to provide blank CD/DVDs for sale to the public.

27. Is a fee to be charged for use of NARA's electronic transfer site?

No, the cost of the electronic transfer is included in the price of a reproduction.

28. How should I charge for the digitization of NARA-made digitized/digital reproductions?

a. The minimum order fee applies to remote orders (fax, email, postal), but not self-service reproductions.

b. The minimum order fee applies to all other orders under $20.00, except for Draft Cards and Naturalization Records. Below are some examples:

Example 1: The customer orders a basic digitized scan of an NATF Form 85: Pension Application File - Civil War and Later (up to 100 pages), that customer would be charged $80.00, regardless of page count. If the order is larger than 100 pages, the customer would be charged $0.70 per page additional (not the $0.80 per page digitized rate).

Example 2: The mail order customer orders a basic digitized scan of a 15-page document (Form 72). The cost is $20.00. Because the total ($12.00) is less than the minimum order fee of $20.00, the minimum order fee applies and the customer is charged $20.00.

Example 3: The customer orders a basic digitized scan of a 26-page document (Form 72). The cost is $20.80. The order total is greater than the minimum order.

Example 4: The customer orders two basic digitized scans of accessioned draft cards. The cost is $14.00. The order total is under $20.00; however, accessioned draft cards and accessioned naturalization records are exempt from the minimum order. WWI era draft cards are available via the online ordering system. All other draft card orders must be ordered through NPRC.

Example 5: The customer orders a basic digitized scan of a six (6) foot long map. The cost is $21.00 ($3.50 per linear foot).

Example 6: The customer orders ten (10) born-digital files, the price to the customer would be $170.00 ($17.00 per file times 10 files).

Example 7: The customer orders 12 born-digital files, the price to the customer would be $168.00 ($14.00 per file times 12 files). Born-digital records are priced at $17.00 per file up to 10 and $14.00 per file for order of greater than 10 files.

Example 8: For an on-site customer, the customer orders a basic digitized scan of a one foot long map. The cost of the copy is $3.50. If this customer were receiving the same order by mail, the $20.00 minimum order reproduction would apply.

Example 9: The customer orders a 4-linear foot, NARA enhanced scan. The cost is $100.00

Example 10: The mail order customer orders 15 NARA-made digitized reproductions of Photographic Film Negatives. The cost is $37.50. Because the total ($37.50) is more than the minimum order fee of $20.00, the minimum order fee does not apply.

Example 11: The customer orders a basic digitized scan of a 26-page document (Form 72), to be delivered via electronic transfer. The cost is $20.80. The order total is greater than the minimum order.

29. When do I use the digitization item numbers as opposed to the paper-to-paper (digitized) item numbers?

In most cases, the paper-to-paper (digitized) item numbers should be used. The "rule of thumb" is: if the record is textual, use the paper-to-paper item number; if the item is non-textual, use the digitized item number. Some examples are shown below:

Example 1: The customer orders a digitized NATF Form 85: Pension Application File - Civil War and Later (up to 100 pages); the item number to be used is *FORM85D*.

Example 2: The customer orders a digitized Naturalization Record, the item number to be used is *FORMNATZ*.

Example 3: The customer orders a basic digitized copy of a five foot long map; the item number to be used is *RS0030*.

Example 4: The customer orders an 11" x 17" NARA Enhanced scan of a photograph; the item number to be used is *RSXC0020*.

30. Are any reproductions excluded from being digitized?

The following products are not currently available to be digitized:

a. Archival Official Military Personnel Files (OMPFs).

b. Archival Official Personnel Folders (OPFs).

c. Motion pictures.

d. Any record requiring certification and/or NARA seal embossing.

31. How do I provide a digitized certification or digitized NARA seal impression to a customer?

Currently, NARA cannot offer digitized certifications or digitized NARA seal impressions. When a customer places an order for a digitized reproduction via the online ordering system, the certification option automatically is removed.

32. How is a "file" unit determined when calculating the cost of a reproduction order for born-digital reproductions?

Because files of differing types of electronic records are structured differently (usually organized by agencies to best suit their own business needs, as well as by type) the only commonality to what constitutes a digital file is that each file is an aggregation of bytes that computer software recognizes as a single entity. A file unit of accessioned born-digital files is determined by how the records of the file were organized by the agency when transferred to NARA or how NARA organized them for preservation purposes.

Appendix A

NARA Reproduction Fee Schedule as of November 6, 2015
See 36 CFR part 1258 for the complete fee schedule regulation.

Product/Service	***Fee***
Record certification (*Record certification is an add-on service, the cost of which is not used to determine minimum reproduction order fees. Certifications will be charged per 150 pages certified.)*	$15.00 per certification
NARA Seal Embossing	$2.50 per seal
Minimum reproductions order *(25 pages or less at the $.80 rate.)*	$20.00
Expedited shipping	$30.00 per order

Self-Service	***Fee***
Self-service paper to paper	$0.25 per copy
Self-service scan	$0.25 per scan
Self-service microform to paper	$0.40 per copy
Self-service microform to digitized	$0.40 per scan
Self-service photo to photo (DC only)	$11.00 per copy
Self-service video copying session with tape (DC only)	$10.00 per session
--Additional session	$6.50 per session
--Additional tape	$3.00 per tape
Blank DVD and sleeve	$2.00
Self-service color paper to paper (DC only)	$1.35 per copy
Self-service book to paper (DC only)	$0.85 per copy

NARA Reproduction Services *(minimum reproduction order fees may apply)*	***Fee***
Paper to paper (or CD/DVD) (up to and including 11" x 17")	$0.80 per copy
Electrostatic copies (22" x 34"), paper to paper	$3.50 per copy
Red line copies	$5.00 per copy
Oversized and per linear foot black-and-white electrostatic copies, paper to paper	$3.50 per linear foot
Oversized and per linear foot color electrostatic copies, paper-to-paper	$5.00 per linear foot
Microfilm or microfiche to paper	$3.50 per copy
Microform to digitized	$4.00 per scan
Paper to microfilm	$2.50 per image
Color paper to paper	$4.60 per copy
Black-and-white negative – 8" x 10"	$18.15 per image
Color negative – 4" x 5"	$22.75 per image
Black-and-white photo print – 8" x 10"	$17.00 per image

NW: 15596 DocId: 70098830 Page 24

Color photo print – 8" x 10"	$22.75 per image
Black-and-white photo print – 11" x 14"	$22.75 per image
Color photo print – 11" x 14"	$28.50 per image
Black-and-white photo print – 16" x 20"	$28.50 per image
Color photo print – 16" x 20"	$40.00 per image
Color transparency – 4" x 5"	$28.50 per image
Color transparency – 8" x 10"	$33.45 per image

Digitized/Digital NARA Reproduction Services *(minimum order fees may apply)*	
Self-service scan	$0.25 per scan
Digitized reproductions of photographic film negatives	$2.50 per scan
Basic digitized scan – up to 8 ½" x 14"	$0.80 per scan
Basic digitized scan – oversized (greater than 8 ½" x 14" up to 22" x 34")	$3.50 per scan
Basic digitized scan –per linear foot	$3.50 per linear ft
NARA enhanced scan – up to 8 ½" x 14"	$20.00 per scan
NARA enhanced scan – oversized (greater than 8 ½" x 14" up to 22" x 34")	$25.00 per scan
NARA enhanced scan – per linear foot	$25.00 per linear ft
Born-digital files, 10 or fewer files	$17.00 per file
Born-digital files, 11 or more files	$14.00 per file

Fixed-Fee Orders *(Fixed-fee order prices supersede digitized reproduction prices (i.e., a Form 82 digitized order carries a fee of $20.00 not a per copy price).)*	***Fee***
NATF Form 81: Order for Copies of Ship Passenger Arrival Records	$20.00 per case
NATF Form 82: Order for Copies of Federal Census Records	$20.00 per case
NATF Form 83: Order for Copies of Eastern Cherokee Application Files	$20.00 per case
NATF Form 84: Order for Copies of Land Records	$50.00 per case
NATF Form 85: Order for Copies of Federal Pension or Bounty Land Warrant Applications	
Full Pension Application File – Pre-Civil War	$55.00 per case
Full Pension Application File – Civil War and Later (up to 100 pages)	$80.00 per case
Full Pension Application File – (each additional page after 100, quote provided to customer)	$0.70 per copy
Pension Documents Packet	$30.00 per case
Bounty Land Warrant Application	$30.00 per case
NATF Form 86: Order for Copies of Military Service Files	$30.00 per case
Accessioned Draft Registration Card *(minimum reproductions order does not apply)*	$7.00 per file
Certified Accessioned Draft Registration Card	$22.00 per file
Accessioned Naturalization Record *(minimum reproductions order does not apply)*	$10.00 per file
Official Military Personnel Files (OMPFs)	
Archival Official Military Personnel Files (OMPFs), 6 or more pages	$70.00 per package

NW: 15596 DocId: 70098830 Page 25

Archival Official Military Personnel Files (OMPFs), 5 or fewer pages	$25.00 per package
Archival Official Military Personnel Files (OMPFs), per page *(minimum reproduction order fees may apply)*	$0.80 per copy
Official Personnel Files (OPFs)	
Archival Official Personnel Folders (OPFs), 6 or more pages	$70.00 per package
Archival Official Personnel Folders (OPFs), 5 or fewer pages	$25.00 per package
Digitized Reproductions of Persons of Exceptional Prominence (PEP) Folders	
Digitized Reproductions of Persons of Exceptional Prominence (PEP) – up to 100 pages	$20.00 per DVD
Digitized PEP – 101 to 300 pages	$40.00 per DVD
Digitized PEP – 301 to 600 pages	$60.00 per DVD
Digitized PEP – 601 to 1,000 pages	$90.00 per DVD
Digitized PEP– 1,001 to 1,800 pages	$150.00 per DVD
Digitized PEP – 1,801 or more pages	$250.00 per DVD
Digitized PEP – Single Folder	$20.00 per DVD

Record Center Court File Packages	***Fee***
NATF Form 90: Order for Copies of Bankruptcy Cases	
Pre-Selected Documents	$35.00 per package
Entire Bankruptcy Case File	$90.00 per package*
NATF Form 91 : Order for Copies of Civil Cases	
Pre-Selected Documents	$35.00 per package
Entire Civil Case File	$90.00 per package*
NATF Form 92: Order for Copies of Criminal Cases	
Pre-Selected Documents	$35.00 per package
Entire Criminal Case Files	$90.00 per package*
NATF Form 93: Order for Copies of Court of Appeals Cases	
Entire Court of Appeals Case	$90.00 per package*
Court Docket Sheet	$35.00 per package

** The price for entire case files that exceed 150 pages will be $90.00 plus a standard labor charge billed in 15-minute increments ($22.00 per 15 minutes, quoted to customer).*

Microform and Digitized Microform Publications	***Fee***
Microfilm publication black-and-white 35 mm or 16 mm roll, US shipping	$125.00 per roll
Microfilm publication black-and-white 35 mm or 16 mm roll, international shipping	$135.00 per roll
Digitized microfilm publication black-and-white 35 mm or 16 mm roll, US shipping	$125.00 per roll
Digitized microfilm publication black-and-white 35 mm or 16 mm roll, international shipping	$135.00 per roll
Digitized microfilm electronic transfer (domestic and international)	$125.00 per roll
Microfiche publication/duplication, US shipping	$12.00 per fiche

NW: 15596 DocId: 70098830 Page 26

Microfiche publication/duplication, international shipping	$22.00 per fiche
Digitized microfiche publication/duplication –electronic transfer (domestic and international)	$12.00 per fiche
Digital publication, US shipping	$55.00 per DVD
Digital publication, international shipping	$65.00 per DVD

Archival Handling Fees *(add to vendor fee)*	***Fee***
Still Photo Item (Washington, DC — also see note below)	$9.50 per item
Cartographic Item (Washington, DC)	$9.00 per item
Motion Picture/Video Item (Washington, DC)	$17.25 per item
Audio Item (Washington, DC)	$6.50 per item
Archival Facility in the Field Still Photo Item	$8.25 per item

Note: For still photo items reproduced by the NARA vendor program in the Washington, DC, area, the fee for each item reproduced will be equal to the Washington, DC still photo item archival handling fee plus the vendor fee for the specific reproduction service requested.

Appendix B

NARA Reproduction Items and Prices as of November 6, 2015
(NARA Internal Use Only)

Item #	Product / Service	Fee
	Minimum Charges, Page Counts, Certifications	
FOIA(b)(7) - (E)	Minimum reproductions order	**$20.00**
	MINCHG Paper to paper page count – Contractor (25 pages or less)	**$0.00**
	MINCHG Paper to paper page count – NARA (25 pages or less)	**$0.00**
	MINCHG Paper to paper page count – NARA (25 pages or less) NRPA	**$0.00**
	MINCHG Micro to paper page count – Contractor (5 pages or less)	**$0.00**
	MINCHG Micro to paper page count – NARA (5 pages or less)	**$0.00**
	MINCHG Paper to paper Color page count – Contractor (4 pages or less)	**$0.00**
	MINCHG Paper to paper Color page count – NARA (4 pages or less)	**$0.00**
	MINCHG Oversize copies page count – Contractor (5 pages or less)	**$0.00**
	MINCHG Oversize copies page count – NARA (5 pages or less)	**$0.00**
	MINCHG Paper to micro page count – Contractor (8 pages or less)	**$0.00**
	MINCHG Paper to micro page count – NARA (8 pages or less)	**$0.00**
	MINCHG WWI Draft Registration Card	**$0.00**
	MINCHG WWII Draft Registration Card	**$0.00**
	MINCHG Naturalization Record	**$0.00**
	NARA Seal Embossing	**$2.50**
	Record Certification (RL) (per 150 pages certified)	**$15.00**
	Record Certifications (Record Centers) (per 150 pages certified)	**$15.00**
	Record Certification (Archival) (per 150 pages certified)	**$15.00**
	Self Service	
	Paper to Paper/Scan (All but DC and College Park)	**$0.25**
	Paper to Paper/Scan (RL)	**$0.25**
	Paper to Paper/Scan (DC and College Park)	**$0.25**
	Microfilm to Paper	**$0.40**
	Microfilm to Paper (RL)	**$0.40**
	Microfilm to Digitized	**$0.40**
	Paper to Paper – Color	**$1.35**
	Book to Paper	**$0.85**

NW: 15596 DocId: 70098830 Page 28

FOIA(b)(7) - (E)

Initial Video Session	**$10.00**
Additional Video Session	**$6.50**
Additional Video Tape	**$3.00**
Blank DVD and Sleeve	**$2.00**
Reproduction Services	
Paper to Paper (or CD/DVD) made by NARA	**$0.80**
Paper to Paper made by NARA - Record Ctrs	**$1.00**
Paper to Paper made by NARA - St. Louis Only	**$0.80**
Paper to Paper made by contractor	**$0.80**
1812 Pension -- Paper to Digitized Copy by GoCo	**$0.50**
Paper to Paper - Color by NARA	**$4.60**
Per Linear Foot Electrostatic Copies	**$3.50 per linear ft**
Per Linear Foot Electrostatic Copies	**$5.00 per linear ft**
Electrostatic Copies (22"x34")	**$3.50**
Red Line Copies	**$5.00**
Microform to Paper	**$3.50**
Microform to Digitized	**$4.00**
Microform to Paper (RL)	**$3.50**
Paper to Microfilm 16mm	**$2.50**
Paper to Microfilm 35mm	**$2.50**
Microfiche duplication domestic	**$12.00**
Microfiche duplication international	**$22.00**
Microfiche publication	**$12.00**
Microfiche publication-international	**$22.00**
Microfiche publication electronic transfer	**$12.00**
Microfiche duplication electronic transfer	**$12.00**
Microfilm publication-silver negative NARA	**$35.00**
Microfilm publication-silver positive NARA	**$35.00**
Digital microfilm (DVD) - NARA	**$55.00**
Digitial microfilm – electronic transfer - NARA	**$55.00**
Microfilm publication silver positive	**$125.00**
Microfilm publication silver positive-international	**$135.00**
Digital microfilm electronic transfer – domestic and international	**$125.00**
Digital microfilm publication (DVD)	**$125.00**
Digital microfilm publication (DVD)- international	**$135.00**
Digital Publication	**$55.00**
Digital Publication - international	**$65.00**

FOIA(b)(7) - (E)

Expedited Shipping	**$30.00**
iArchives Shipping and Handling	**$10.00**
Form 80 Series, Draft Cards, Naturalization Records	
81 – Ship Passenger Arrival Records	**$20.00**
81 – w/ Certification	**$35.00**
82 – Census Records	**$20.00**
82 – w/ Certification	**$35.00**
83 – Eastern Cherokee Applications	**$20.00**
84 – Land Entry Files	**$50.00**
85A – Full Pension Application File (Non-Civil War)	**$55.00**
85B – Pension Documents Packet	**$30.00**
85C – Bounty Land Warrant Application	**$30.00**
85D – Full Pension Application File (Civil War ≤ 100 pgs)	**$80.00**
85D – Additional pages after 100 (NARA Made)	**$.70 / page**
85D – Additional pages after 100 (Contractor Made)	**$.70 / page**
86 – Military Service Records	**$30.00**
Naturalization Record	**$10.00**
Naturalization Record - certified	**$25.00**
WWI Draft Registration Card	**$7.00**
Certified WWI Draft Registration Card	**$22.00**
WWII Draft Registration Card	**$7.00**
Form 90 Series	
Bankruptcy cases pre-selected	**$35.00**
Bankruptcy cases pre-selected – certified	**$50.00**
Bankruptcy cases file (up to 150 pages, then $22 per 15 minutes)	**$90.00**
Bankruptcy cases file - certified (up to 150 pages, then $22 per 15 minutes)	**$105.00**
Bankruptcy Docket Sheet	**$35.00**
Bankruptcy Docket Sheet - certified	**$50.00**
Civil case file - certified (up to 150 pages, then $22 per 15 minutes)	**$105.00**
Civil case docket sheet	**$35.00**
Civil case docket sheet - certified	**$50.00**
Criminal cases pre-selected	**$35.00**
Criminal cases pre-selected - certified	**$50.00**
Criminal cases file (up to 150 pages, then $22 per 15 minutes)	**$90.00**
Criminal cases file - certified (up to 150 pages, then $22 per 15 minutes)	**$105.00**
Criminal case docket sheet	**$35.00**

Criminal case docket sheet - certified	**$50.00**
Court of Appeals file (up to 150 pages, then $22 per 15 minutes)	**$90.00**
Court of Appeals file - certified (up to 150 pages, then $22 per 15 minutes)	**$105.00**
Court of Appeals docket sheet	**$35.00**
Court of Appeals docket sheet - certified	**$50.00**
Court file page count for all FRCs – must use for Form 90s	**$0.00**
Standard labor charge after 150 pages (Form 90s only)	**$22.00**
Other – St. Louis	
Pull and Refile fee	**$15.00**
Official Military Personnel Files (OMPFs)	
OPMF – Official Military Personnel File – St. Louis – 6 or more pages	**$70.00**
OMPF – Official Military Personnel File – St. Louis – 5 or fewer pages	**$25.00**
OMPF – Official Military Personnel File – St. Louis – Per page	**$0.80**
Official Personnel Files (OPFs)	
Official Personnel Folder – 6 or more pages	**$70.00**
Official Personnel Folder – 5 or fewer pages	**$25.00**
Digitized Reproductions of Persons of Exceptional Prominence (PEP) Folders	
Digitized PEP – Tier 1 – up to 100 pages	**$20.00**
Digitized PEP – Tier 2 – 101 to 300 pages	**$40.00**
Digitized PEP – Tier 3 – 301 to 600 pages	**$60.00**
Digitized PEP – Tier 4 – 601 to 1,000 pages	**$90.00**
Digitized PEP – Tier 5 – 1,001 to 1,800 pages	**$150.00**
Digitized PEP – Tier 6 – 1,801 or more pages	**$250.00**
Digitized PEP – Single Folder	**$20.00**
Court file page count for all FRCs – must use for Form 90s	**$0.00**
NARA-Certification-AFN-C	**$2.00**
OPM-No Fee copies-AFN-C	**$0.00**
OPM-Search&Review-com-AFN-C	**$14.25**
OPM-Add'l copies-other-AFN-C	**$0.13**
Mil/Med-Search under hour-AFN-M	**$8.30**
Mil/Med-Search per hour-AFN-M	**$13.25**
Mil/Med-Copies 1-6-AFN-M	**$3.50**
Mil/Med-Add'l copies-AFN-M	**$0.10**
Mil/Med-Certification-AFN-M	**$5.20**
DOD-No Fee search-AFN-M	**$0.00**
DOD-Full Chg-Search under hour-AFN-M	**$8.30**

FOIA(b)(7) - (E)

	DOD-Full Chg-Search per hour-AFN-M	**$13.25**
	DOD-Full Chg-Copies 1-6-AFN-M	**$3.50**
	DOD-Full Chg-Add'l copies-AFN-M	**$0.10**
	DOD-Certification-AFN-M	**$5.20**
	DOD-Partial Chg-Copies 1-6 - AFN-M	**$3.50**
	DOD-Partial Chg-Add'l copies-AFN-M	**$0.45**
	DOD-Partial Chg-Packages-AFN-M	**$5.20**
	Digital Reproductions	
	Self-service scan	**$0.25**
	Basic digitized scan – up to 8 ½" x 14"	**$0.80**
	Basic digitized scan – oversized (greater than 8 ½" x 14" up to 22" x 34")	**$3.50**
	Basic digitized scan –per linear foot	**$3.50 per linear ft**
	Digitized reproductions of photographic film negatives	**$2.50**
	NARA enhanced scan – up to 8 ½" x 14"	**$20.00**
	NARA enhanced scan – oversized (greater than 8 ½" x 14" up to 22" x 34")	**$25.00**
FOIA(b)(7) - (E)	NARA enhanced scan – per linear foot	**$25.00 per linear ft**
	Born-digital files up to 10 files	**$17.00 / file**
	Born-digital files, 11 files and up	**$14.00 / file**
	Vendor and Photo Items	
	Cartographic item	**$9.00**
	Certification	**$15.00**
	Still picture item	**$9.50**
	Motion picture item	**$17.25**
	Audio item	**$6.50**
	Photo to Photo copy	**$11.00**
	BW negative 4x5	**$15.85**
	BW negative 8x10	**$18.15**
	Color negative 4x5	**$22.75**
	BW photo print 8x10	**$17.00**
	Color photo print 8x10	**$22.75**
	BW photo print 11x14	**$22.75**
	Color photo print 11x14	**$28.50**
	BW photo print 16x20	**$28.50**
	Color photo print 16x20	**$40.00**
	Color 4x5 transparency	**$28.50**
	Color 8x10 transparency	**$33.45**

FOIA(b)(7)-(E)

Arch handling-photo	**$8.25**
Photo Vendor Chg	**$2.00**
BW negative 4x5	**$18.00**
BW RC print 8x10-1st	**$14.00**
Thomson Reuters	
Thomson Reuters	**$57.50**
Thomson Reuters	**$3.75**
Thomson Reuters	**$4.25**
Thomson Reuters	**$4.00**
Thomson Reuters	**$4.10**
Thomson Reuters	**$0.90**
Thomson Reuters	**$0.90**
Thomson Reuters	**$4.25**