



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Two (2) Centers for Disease Control and Prevention (CDC) Information Security Guides, 2005-2009

Requested date: 10-February-2020

Release date: 26-February-2020

Posted date: 13-April-2020

Source of document: FOIA Request  
CDC/ATSDR  
Attn: FOIA Office, MS-D54  
1600 Clifton Road, NE  
Atlanta, GA 30333  
Fax: (404) 235-1852  
Email: [FOIARequests@cdc.gov](mailto:FOIARequests@cdc.gov)

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and 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.



Centers for Disease Control  
and Prevention (CDC)  
Atlanta GA 30333

February 26, 2020

Via email

This letter is our final response to your Centers for Disease Control and Prevention and Agency for Toxic Substances and Disease Registry (CDC/ATSDR) Freedom of Information Act (FOIA) request of February 10, 2020, assigned #20-00599-FOIA, for , "A copy of two CDC documents: CDC-IS-2002-03 and CDC-IS-2005-02".

The Strategic Business Initiatives Unit located 66 pages of responsive records. After a careful review of these pages, no information was withheld from release.

If you need any further assistance or would like to discuss any aspect of the records provided please contact either our FOIA Requester Service Center at 770-488-6399 or our FOIA Public Liaison at 770-488-6277.

Sincerely,

A handwritten signature in black ink, appearing to read "Roger Andoh".

Roger Andoh  
CDC/ATSDR FOIA Officer  
Office of the Chief Operating Officer  
(770) 488-6399  
Fax: (404) 235-1852

20-00599-FOIA

Manual Guide - Information Security CDC-02

Date of Issue: 07/22/2005

Proponents: Office of Security and Emergency Preparedness

## SENSITIVE BUT UNCLASSIFIED INFORMATION

Sections	I. <a href="#">PURPOSE</a>
	II. <a href="#">BACKGROUND</a>
	III. <a href="#">SCOPE</a>
	IV. <a href="#">ACRONYMS AND DEFINITIONS</a>
	V. <a href="#">POLICY</a>
	VI. <a href="#">PROCEDURES</a>
	VII. <a href="#">RESPONSIBILITIES</a>
	VIII. <a href="#">REFERENCES</a>

### [Exhibit 1: Common Information Types with Sensitivity Guidance](#)

### [Exhibit 2: Summary Listing of Common Information Types](#)

#### I. PURPOSE

The purpose of this document is to provide policy and procedures to the Centers for Disease Control and Prevention<sup>[1]</sup> (CDC) that allow for the accomplishment of our public health service mission while safeguarding the various categories of unclassified data and document information that, for legitimate government purposes and good reason, shall be withheld from distribution or to which access shall be denied or restricted.

#### II. BACKGROUND

There are various categories of information, data and documents that are sensitive enough to require protection from public disclosure for one or more reasons outlined under the exemptions of the Freedom of Information Act but may not otherwise be designated as national security information.

#### III. SCOPE

This policy applies to all individuals, employees, fellows, attached uniform service members, Public Health Service Commissioned Corps, Department of Defense employees and service members, contractors and subcontractors working at CDC, or under the auspices thereof.

#### IV. ACRONYMS AND DEFINITIONS

##### A. For the purposes of this policy, the following acronyms apply.

1. **CARI:** Contractor Access Restricted Information
2. **CSASI:** Computer Security Act Sensitive Information
3. **CUI:** Controlled Unclassified Information
4. **DCO:** document control officer
5. **DEA-S:** Drug Enforcement Agency Sensitive
6. **DOD:** Department of Defense
7. **DOE-OUO:** Department of Energy Official Use Only
8. **DOS-SBU:** Department of State Sensitive But Unclassified
9. **EO:** Executive Order
10. **FOIA:** Freedom of Information Act



- 11. **FOUO:** For Official Use Only
- 12. **GSA:** General Services Administration
- 13. **GSA-SBU-BI:** GSA Sensitive But Unclassified Building Information
- 14. **HHS:** Department of Health and Human Services
- 15. **ITAR:** International Traffic in Arms Regulations
- 16. **LES:** Law Enforcement Sensitive
- 17. **LOU:** Limited Official Use
- 18. **OSEP:** Office of Security and Emergency Preparedness
- 19. **OSPI:** Operations Security Protected Information
- 20. **PAPI:** Privacy Act Protected Information
- 21. **PHS:** Public Health Service
- 22. **PROPIN:** proprietary information
- 23. **SASI:** Select Agent Sensitive Information
- 24. **SBU:** Sensitive But Unclassified
- 25. **SDD:** Security and Drug Testing Program Division
- 26. **SNM:** Special Nuclear Material
- 27. **UCNI:** Unclassified Controlled Nuclear Information

**B. For the purposes of this policy, the following definitions apply.**

**1. Sensitive But Unclassified**

This designation is applied to unclassified information that may be exempt from mandatory release to the public under FOIA. SBU is the formal designation for information that by law or regulation requires some form of protection but is outside the formal system of classification, as in accordance with Executive Order 12958, as amended. There are currently 13 types or categories of SBU, established to allow for specific administrative methods and procedures: CSASI, CARI, CUI, DEA-S, DOE-OUO, DOS-SBU (formerly known as LOU), FOUO, GSA-SBU-BI, LES, OSPI, PAPI, SASI, and UCNI.

**2. Computer Security Act Sensitive Information**

"Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section [552a of Title 5, USC](#) (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." Reference Public Law 100-235, The Computer Security Act of 1987, which is concerned with protecting the availability and integrity as well as the confidentiality of information.

**3. Contractor Access Restricted Information**

Unclassified information that involves functions reserved to the federal government as vested by the Constitution as inherent power or as implied power as necessary for the proper performance of its duties. In many instances, CARI prevents contractors from making decisions that would affect current or future contracts and procurement procedures, primarily during pre-award activities. CARI maximizes competition for government requirements and encourages absolute integrity in all dealings with the private sector while promoting economy, efficiency and effectiveness. See Acquisition Management Policy CDC-10, [Procurement Integrity Restrictions](#).

**4. Controlled Unclassified Information**

DOD unclassified information that requires application of controls and protective measures for a variety of reasons other than national security information (that has been classified in accordance with [EO 12958](#), as amended, or any precursory executive orders). Policy and procedures for CUI are found in and are in accordance with DOD Regulation 5200.1-R, The Information Security Program.



## **5. DEA Sensitive**

DEA Sensitive is unclassified information that is originated by DEA and requires protection against unauthorized disclosure in order to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The administrator and certain other officials of the DEA have been authorized to designate information as "DEA SENSITIVE."

## **6. Department of State Sensitive But Unclassified**

Unclassified information that originated within the Department of State which warrants a degree of protection or administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA. Prior to 26 January 1995, this information was designated and marked LOU. The LOU designation will no longer be used.

## **7. DOE Official Use Only**

The Department of Energy designation for information that is sensitive but unclassified and is, or should be, exempt from public release under FOIA.

## **8. Export Controlled Information (or material)**

Information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State. This pertains to items controlled by the ITAR, or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export Controlled Information must be controlled as **◆ Sensitive But Unclassified ◆** information and marked accordingly. A large, frequently updated database of information on export administration regulations is available at [http://www.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html).

## **9. The Arms Export Control Act**

Act which regulates the export of defense articles and services. Such exports may be licensed only if their export will strengthen United States national security, promote foreign policy goals, or foster world peace. The Arms Export Control Act is administered by the Department of State, Center for Defense Trade Controls, through the ITAR and the United States Munitions List (defense articles that require a license prior to export).

## **10. The Export Administration Act**

Act which regulates the export of dual-use items (those that have both a military and civilian use). Dual-use items that would make a significant contribution to the military potential of another country are on the Department of Commerce's Commodity Control List, and a license is required for their export. The Commodity Control List includes items from the Defense Department's Military Critical Technology List and technology that could support the proliferation of chemical, biological or nuclear weapons or missile technology. A recent study of illegal technology transfer operations directed against the United States identified 56 different end-user countries.

## **11. For Official Use Only**

A designation that is applied to unclassified information that is exempt from mandatory release to the public under FOIA. FOIA specifies nine categories of information that can be withheld from public (see definition below). Information that is currently and properly classified can be withheld from mandatory release under the first exemption category (subparagraph (a) below). FOUO is applied to information which is exempt under one of the other eight categories.

## 12. Freedom of Information Act

This requires the release of publicly requested information with several exceptions:

- (a) Information that is currently and properly classified.
- (b) Information that pertains solely to the internal rules and practices of the agency and, disclosure would allow circumvention of agency regulations.
- (c) Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- (d) Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.
- (e) Intra-agency memoranda that are deliberative in nature ♦ this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
- (f) Information for which the release could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- (g) Records or information compiled for law enforcement purposes that:
  - (1) could reasonably be expected to interfere with law enforcement proceedings;
  - (2) would deprive a person of a right to a fair trial or impartial adjudication;
  - (3) could reasonably be expected to constitute an unwarranted invasion of personal privacy of others;
  - (4) discloses the identity of a confidential source;
  - (5) discloses investigative techniques and procedures; or
  - (6) could reasonably be expected to endanger the life or physical safety of any individual.
- (h) Certain records of agencies responsible for supervision of financial institutions.
- (i) Geological and geophysical information concerning wells.

## 13. GSA Sensitive But Unclassified Building Information

Information concerning General Services Administration Public Building Services controlled space including owned, leased or delegated Federal facilities. GSA-SBU-BI includes building designs such as floor plans, construction plans and specifications, renovation/alteration plans, equipment plans and locations, building operating plans, information used for building services contracts and/or contract guard services, or any other information considered a security risk, such as, but not limited to:

- (a) Locations of secure functions in the facility, such as VIP offices and conference rooms, security areas, childcare, major computer processing or equipment rooms;
- (b) Location of all utilities, such as heating, ventilation, air conditioning, information technology systems, location of air intake vents, water sources, gas lines, plumbing lines, building automation systems, power distribution systems, emergency generation equipment, uninterruptible power sources, security and fire alarm systems/routes and annunciation panels;



(c) Location and type of structural framing for the building and any information regarding structural analysis, or building security and blast mitigation analysis and counter terrorism methods taken to protect the occupants and building; and

(d) Information regarding security systems or strategies of any kind (such as camera locations) or security guards (such as number and location). References: GSA PBS 3490.1 of March 8, 2002, GSA Order Safeguarding Sensitive Unclassified Information (ADM 1800.3B); Instructional Letter CIO IL-99-1, Safeguarding Sensitive Unclassified Information; and GSA Acquisition Manual (GSAM) (ADP P2800.12B).

#### **14. Law Enforcement Sensitive**

A designation and marking for records or information compiled for law enforcement purposes that the release of:

- (a) could reasonably be expected to interfere with law enforcement proceedings;
- (b) would deprive a person of a right to a fair trial or impartial adjudication;
- (c) could reasonably be expected to constitute an unwarranted invasion of personal privacy of others;
- (d) disclose the identity of a confidential source;
- (e) disclose investigative techniques and procedures; or
- (f) could reasonably be expected to endanger the life or physical safety of any individual.

#### **15. Operations Security Protected Information**

Unclassified information concerning CDC mission, functions, operations, or programs that require protection in the national interest, security or homeland defense as iterated in National Security Decision Directive 298, January 1988, which established a National Operations Security Program.

#### **16. Privacy Act Protected Information**

Information that if released could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals. Additional guidance may be found in the Privacy Act of 1974, [5 USC 552a](#), [45 CFR Part 5b](#), and in General Administration Policy [CDC-63, Privacy Act](#).

#### **17. Proprietary Information**

Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.

#### **18. Select Agent Sensitive Information**

The portion of the National Laboratory Registration and Select Agent Program information that has been determined by the HHS Original Classification Authority to be sensitive but unclassified and is prohibited from public disclosure by Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002. See also [42 USC 247d-6b\(d\)](#).



Classification Guidance:

HHS has classified the Select Agent Program electronic and document database. This database contains information concerning the possession, use, or transfer of select biological agents and toxins as required by 42 CFR Part 73 and 43 CFR 72.6. The Select Agent Program electronic and document database, and any portion of that database, which contains information concerning more than one entity, is classified as SECRET.

Any document that has been prepared using information from the Select Agent Program database, which identifies more than one entity as having a specific select agent or agents, is classified as SECRET.

Any document that has been prepared using information from the Select Agent Program database which identifies more than one entity as having an unspecified select agent or agents, is classified as CONFIDENTIAL.

A portion of the Select Agent Program database, or any document that has been prepared using information from the Select Agent Program database, which is limited to information received from one entity will be unclassified but will be protected to safeguard the public interest and marked as FOR OFFICIAL USE ONLY. It would be inappropriate to give such material to persons outside Federal agencies without the consent of a responsible HHS official.

Cover sheet marking for Select Agent Sensitive Information (SASI):

"This document is intended for the exclusive use of the recipient(s) named above. It may contain sensitive information that is protected, privileged, or confidential, and it should not be disseminated, distributed, or copied to persons not authorized to receive such information. If you are not the intended recipient(s), any dissemination, distribution, or copying is strictly prohibited. If you think that you have received this document in error, please notify the sender immediately and destroy the original."

**19. Unclassified Controlled Nuclear Information**

Unclassified information on aspects of security, including security plans, procedures, methods/measures, and equipment, for the physical protection of DOD SNM, equipment, and facilities. Information is designated DOD UCNi only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security, by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DOD SNM, equipment, or facilities.

**V. POLICY**

All CDC employees and otherwise affiliated persons shall protect Sensitive But Unclassified information by following the procedures contained in this policy document and/or related policies of the CDC, HHS, Executive Orders, other presidential directives, United States Federal Court rulings, and applicable laws of the United States of America.

Policies and Procedures for the protection of National Security Information (Classified Information) are marked as Confidential, Secret, or Top Secret in accordance with Executive Order 12958, as amended, and can be found in other CDC and HHS documents (see section VIII. References of this policy for specific citations).

**VI. PROCEDURES****A. Review and Approval of Information Prior to Public Release**

A process has been established for review and approval of all information including hard copies and

digital publications prior to its public release. The OSEP has appointed a DCO who is authorized to review and approve information for release and to clear policies and procedures for posting web site content. The DCO is further authorized to make sensitivity determinations ensuring that certain information is not for public release (subject to the FOIA officer), and that the information should be marked as SBU.

However, marking information SBU does not automatically qualify it for a public release exemption. If a public request for a SBU document is received, the information should be reviewed to determine if it actually qualifies for exemption. Moreover, the absence of the SBU or other related marking does not necessarily mean the information should be publicly released. Some types of records (e.g., most human resources and financial information) are not normally marked SBU but may still qualify for withholding under FOIA, unless otherwise authorized for release by the individual. Therefore, all information should be reviewed and approved prior to its public release.

To protect against the unauthorized disclosure of classified information, all CDC employees and otherwise affiliated persons are required to submit for sensitivity review any material intended for public release that might be based in any way on information learned through access to classified information. This requirement covers all written materials including technical papers, books, articles, and manuscripts lectures, speeches, films, and videotapes.

The requirement for a sensitivity review applies equally to hard-copy and electronic documents. Electronic documents that require sensitivity review include, but are not limited to, submissions to online publications, documents that are drafted or stored on a publicly accessible home page, and submissions to another Internet site, regardless of site or location.

For some persons with access to Sensitive Compartmented Information (SCI) or a DOD Special Access Program (SAP), the requirement for pre-publication review may extend to resumes and curriculum vitae that identify specific tasks performed while holding the clearance.

When any portion of the information proposed for disclosure "might" be covered by a signed nondisclosure agreement, CDC employees and otherwise affiliated persons may not take any steps toward public disclosure until receiving written permission to do so. This is a lifetime obligation that remains in effect as long as the information remains classified or sensitive.

The government may take control of all rights, title, and interest in any and all "royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms" of the nondisclosure agreement signed at the time of security clearance acceptance.

## **B. Pre-Publication Review of Web Site Content**

Information on the Internet may be intended for a limited audience; however it actually becomes available to a world wide audience. The World Wide Web was not designed with security in mind, and unencrypted information is at high risk of compromise. CDC OCISO and ITSO guidelines take into account what security access controls, if any, are in effect for specific sites, the sensitivity of the information, and the target audience for which the information is intended.

Most types of SBU information (i.e., DOD Technical Information, FOUO information, export-controlled information, Unclassified Nuclear Information, and Privacy Act information) shall not go on a web site unless that site is protected by encryption. Decisions on the handling of proprietary or trade secret information in the private sector are made by the owners of that information.

SBU information is normally marked with a sensitivity indicator at the time it is created. However, the absence of any sensitivity marking is not a valid basis for assuming that information is non-sensitive. If information could be considered sensitive, it should first be seen by the DCO at the branch level.



CDC sensitivity determinations and classification decisions require that judgments consider the potential consequences of aggregation. The term "sensitive by aggregation" refers to the fact that information on one site may seem unimportant, but when combined with information from other web sites, it may form a larger and more complete picture that was neither intended nor desired. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that site will be accessed by those seeking information that can be used against the government.

There are several common mistakes that people make when deciding what to put on a web site: ignoring the danger associated with personal data on the Internet; assuming that information is not sensitive because it is not marked with a sensitivity indicator; and underestimating the ease and potential significance of aggregation.

Personal information such as: addresses; telephone numbers, other than those readily available to the public; social security numbers; dates of birth; names of family members in biographic summaries, etc; could facilitate criminal, harassment, or terrorist activity against military personnel or government or defense contractor employees and should not be on the Internet.

### **C. Sensitivity/Classification Decision and Notification**

The DCO shall issue a decision within 5 working days as to the sensitivity of information of a draft document. If a decision cannot be made, or if it is determined that the information should be classified, the document will be sent to either a security review panel at OSEP and/or forwarded to HHS/SDD for a classification determination. The originator will be promptly notified as to the status of the document, especially those documents that have been referred to the review panel or to HHS.

### **D. Appeal of Sensitivity/Classification Decision**

Sensitivity determinations may be appealed by a formal written request from the originator through the affected center/office director and sent to the Director of OSEP for a final determination. Appeals regarding classification determinations must follow the formal Classification Challenge Procedures as specified per [EO 12958](#), as amended; the ISOO Implementing Directive of September 2003; and the current HHS National Security Information Manual.

### **E. Types of Sensitive But Unclassified Information**

Sensitive information consists of any information exempted from FOIA and includes, but is not limited to, information related to personnel, security, select agents, and HHS-designated critical national electronic surveillance systems.

Examples include, but are not limited to:

- 1. Personnel.** General personnel information including: evaluation and performance data; security information, including background investigation results and adjudication, and infractions/incident reports; personal information when associated with an individual's work on topics where security is involved (e.g., names and details of those working with select agents, classified data, counterintelligence) or with those individuals who are authorized to have a level of access beyond the average CDC employee, contractor, or visitor.
- 2. Security.** Facility blueprints and other detailed facility information, databases associated with the physical security system, vulnerabilities of such facilities or sensitive information, network security information, security procedures, access codes (combinations or passwords), badge design information, security audit results, physical security performance test results, results of response force exercises, incident reports and disciplinary actions, response force capabilities, and security plans.



**3. Select Agents.** Databases and lab records associated with the select agent program including, but not limited to, inventory databases and chain-of-custody records; select agent transfer records; documentation associated with the unexpected results of an experiment, that if deliberately conducted would be prohibited by [9 CFR 121.10](#); and information deemed too sensitive for public release by a review and approval panel.

## **F. SBU Mandatory Release Exemptions under the Freedom of Information Act (FOIA)**

Information, in either electronic or hard copy form, determined to be sensitive but unclassified should fall within one or more of the eight FOIA exemption categories identified in Section IV (FOIA definition) to be exempt from mandatory release to the public.

## **G. SBU Personnel Access Requirements**

**Access to Sensitive Information.** Sensitive information should only be released to authorized employees who have a specific job-related need-to-know for that information. The final responsibility for determining whether an individual has a need for access to sensitive information should be determined by the individual who has authorized possession, knowledge, or control of the information. Individuals responsible for sensitive information should be authorized to convey such information to others who have an official need-to-know.

## **H. SBU Safeguarding / Storage Requirements**

**1. Protection of Sensitive But Unclassified While In Use.** Reasonable precautions should be taken to prevent access to sensitive information by persons who do not require the information to perform their jobs (e.g., sensitive documents should neither be read in a public place, nor taken home).

**2. Storage Rules for Sensitive But Unclassified.** Sensitive information, both in hard copy and electronic form, should be physically protected and should be stored in limited areas. Exclusion areas and special exclusion areas are also acceptable storage locations, but high containment laboratories should only be used as storage areas for sensitive information when absolutely necessary. Storing sensitive information in a property protection area or a public area is only acceptable if additional protections are taken to increase protection to a level comparable to that in a limited area.

All sensitive information existing in hard copy should be stored within a locked container in a limited or exclusion area, an access controlled electronic environment, or be under the physical control of an authorized individual. When limited or exclusion areas are not available, for instance when an individual is traveling within the United States, a locked container within a locked room will suffice (e.g., locked briefcase or suitcase within a locked hotel room or vehicle). Sensitive information should not be taken outside the United States.

Information handled electronically and transmitted over the network is at a higher risk of being released or altered. Sensitive information stored on the CDC network should be protected at a level that can ensure that only those who are authorized to view the information are allowed access (e.g., machine-generated passwords, encryption). The CDC network systems should maintain a high level of electronic protection (e.g., firewalls, intrusion detection, defense-in-depth, isolation of sensitive information, good practices network administration) to ensure the integrity of sensitive information and to prevent unauthorized access into these systems. Regular review of the protection methods used and system auditing are also critical to maintain protection of these systems.

The physical elements of the network systems which store and transmit sensitive information or that have direct access to sensitive information should be secured within a Limited Area or Exclusion Area. The more central the information resource is (e.g., a network or security system control room) the higher the level of access control that should be applied.

## I. SBU Marking Requirements

**1. Marking Rules for Sensitive But Unclassified.** Information that has been determined to be SBU should be designated as **◆ Sensitive But Unclassified ◆** with the appropriate markings and labels.

**2. Documents.** Documents containing sensitive information should be covered with a **◆ Sensitive But Unclassified ◆** cover page, and the outside of the back cover should be marked **◆ Sensitive But Unclassified ◆**.

Internal pages of the document should be marked **◆ Sensitive But Unclassified ◆** at the top and bottom of each page in letters clearly distinguishable from the text. The acronym SBU may be used when space does not permit spelling out **◆ Sensitive But Unclassified ◆**.

The first page should contain the following statement at the lower left hand corner, and should be completed with the applicable FOIA exemption number(s).

### Sensitive But Unclassified (SBU)

This document contains information that may be exempt from public release under the Freedom of Information Act (FOIA) (5 U.S.C. 552), exemption(s) \_\_\_\_\_ apply. Approval by the Centers for Disease Control and Prevention Document Control Officer (OSEP) and the CDC FOIA Officer, prior to public release via the FOIA Office is required.

**3. Electronic Media.** Electronic media containing sensitive information should be labeled **◆ Sensitive But Unclassified ◆**. The label should be plainly visible and should be applied in a way that it does not interfere with the drive mechanism. Electronic media includes magnetic tape reels, disk packs, diskettes, compact discs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes and micro-cassettes, videotapes, and any other device on which data is stored and which normally is removable from the system by the user or operator. The outer covering for any of the above removable storage media should also be marked **◆ Sensitive But Unclassified ◆**.

Videotapes should also contain **◆ Sensitive But Unclassified ◆** at the beginning and end of the played video, if possible. Audible cassettes, if possible, should contain an audible statement at the beginning and end of the played portion, which informs the listener that the tape contains sensitive unclassified information.

**4. Blueprints, Engineering Drawings, Charts, and Maps.** Blueprints, engineering drawings, charts, and maps containing sensitive information should be marked **◆ Sensitive But Unclassified - Building Information ◆** or "SBU-BI" at the top and bottom of each page. If the blueprints, drawings, charts, or maps are large enough that they are likely to be rolled or folded, **◆ Sensitive But Unclassified - Building Information ◆** should be placed to be visible when the item is rolled or folded.

**5. Photographs and Negatives.** Photographs containing sensitive information should be marked **◆ Sensitive But Unclassified ◆** on the face, if possible. If this cannot be done, the marking should be placed on the reverse side. Negatives, positives, or other film containing sensitive information should be marked **◆ Sensitive But Unclassified ◆** on the film itself if possible, otherwise protected inside a marked container.

## J. Reproduction of Sensitive But Unclassified



SBU Documents may be reproduced without the permission of the originator to the extent necessary to carry out official CDC activities. Copies should be protected in the same manner as originals. In the event of a copy machine malfunction, the copy machine should be cleared and all paper paths checked for papers containing sensitive information.

## **K. SBU Transfer Requirements**

**1. Communicating Sensitive Information.** Sensitive information may be communicated in the following ways:

- ? from person to person in direct contact with one another;
- ? over a land-line telephone;
- ? via first class, priority, or overnight mail;
- ? via fax machine;
- ? via e-mail to and from CDC e-mail addresses ([...][@cdc.gov](mailto:cdc.gov)) that reside completely within the CDC network; or
- ? via e-mail to and/or from an e-mail address outside of the CDC network, provided that the sensitive data is encrypted and authenticated.

**2. Discussing Sensitive Information via Telephone or Video Conference.** Although sensitive information may be discussed on landline telephones, sensitive information should not be discussed on cellular phones. Sensitive information should not be transmitted via open network communication channels, including online video conferencing unless such a conference is held on a restricted network.

**3. Mailing of Sensitive Information.** Transmission of sensitive information should be done in a manner that informs those with a need-to-know of the level of sensitivity while not advertising the fact to the general public. It is also important to use a reliable means of shipping. These considerations help to avoid unauthorized disclosure or dissemination of sensitive information.

**4. Internal Mail.** Before transmitting sensitive information through the CDC internal mail, the information should have appropriate markings and cover sheet and be placed in a **◆ Sensitive But Unclassified ◆** envelope.

**5. External Mail.** Sensitive information sent outside CDC premises should be transmitted via first class mail, priority, or overnight mail. The outer wrapping should not be marked in a manner that would reveal the contents of the envelope or package to unauthorized personnel.

**6. Faxing of Sensitive But Unclassified Information.** Prior to faxing sensitive information, the sender should confirm that an authorized person will be present to accept the transmittal at the receiving end, or the sender should verify that the receiving facility is protected in a manner sufficient to preclude unauthorized access to the transmitted material.

**7. Electronic Transmission.** Sensitive information should be encrypted and authenticated if it is sent from the CDC network to an unsecured (non-CDC) network. Sensitive information should never be communicated over wireless technologies, such as cellular or cordless telephones, or wireless data devices (e.g., Blackberries).

## **L. SBU Disposal / Destruction Requirements and Methods**

### **Destruction of Sensitive Information**

Sensitive information should be destroyed by shredding or burning; paper containing sensitive information should not be recycled.

Deleting, erasing, or formatting will not sufficiently remove sensitive information from electronic storage formats. Instead, files should be removed by using multiple passes (10 times minimum) of a hard drive



wiping program.

Electronic or removable media should be physically damaged to the point of inoperability, via shredding, degaussing, melting, or other such methods before disposal.

#### **M. Enforcement**

A violation of this policy may be cause for administrative action, including, but not limited to, removal from employment or discharge from USPHS Commissioned Corps. Violations of this policy may also result in civil and criminal penalties, including fines and imprisonment, under the laws of the United States.

#### **N. Information Contact**

For additional information about this policy, or to submit a document for sensitivity review or classification determination, contact the OSEP Document Control Officer at 404-639-7650.

### **VII. RESPONSIBILITIES**

#### **A. OSEP responsibilities regarding sensitive but unclassified information**

CDC OSEP shall appoint one or more DCO(s) to implement this policy and procedures. The Director of OSEP shall form an appeal board as needed to render timely judgments concerning appeals to sensitivity determinations. The Director shall forward challenges to classification decisions according to the DHHS Manual on National Security Information.

#### **B. DCO(s) responsibilities regarding sensitive but unclassified information**

DCO(s) shall review all submitted materials and render a sensitivity determination or process same for a national security information classification decision in accordance with this policy and applicable other laws, orders, rules and regulations. Sensitivity determinations and classification decisions and notification shall be documented and in a written form. Files will be maintained in accordance with the CDC Records Control Schedule.

#### **C. Supervisors and Managers responsibilities regarding sensitive but unclassified information**

Supervisors and managers shall ensure that only authorized employees have access to SBU information. They shall annually, and more often as necessary, inform their employees of the need to protect SBU information and of the requirement to have all documents that they create that may contain SBU sent to the DCO(s) for a sensitivity determination. They shall enforce the procedures of this policy among their employees and within the work spaces for which they are responsible. Supervisors shall report suspected or known violations of this policy or procedures to the DCO(s) as soon as possible.

#### **D. Employees and Affiliated Persons responsibilities regarding sensitive but unclassified information**

Employees and affiliated persons shall become knowledgeable of this policy and procedures. They shall comply with the requirements as herein established.

#### **E. CDC FOIA Officer responsibilities regarding sensitive but unclassified information**

CDC FOIA Officer shall obtain a sensitivity determination or classification decision prior to final FOIA decision to release or deny CDC records.

#### **F. CDC OCISO responsibilities regarding sensitive but unclassified information**

CDC OCISO shall provide advice, assistance, policy and technical guidance on information systems security, with emphasis on FISMA 2002, and the Computer Security Act of 1987.

## VIII. REFERENCES

- A. [Arms Export Control Act](#)
- B. [CDC-3, Protection of Information Resources, April 10, 2002](#)
- C. [CDC-5, Classified Material, April 10, 2002](#)
- D. [CDC-8, Employee Use of CDC Information Technology Resources, June 9, 1999](#)
- E. [CDC-10, Procurement Integrity Restrictions, February 21, 2004](#)
- F. [CDC-18, Interim Clearance of Information Products Disseminated Outside CDC for Public Use, June 21, 2005](#)
- G. [CDC-63, Privacy Act, November 30, 2000](#)
- H. [CDC-78, Freedom of Information Act, March 9, 2002](#)
- I. [CDC-83, Export Controls for Biological, Chemical, and Related Technical Data and Equipment, June 6, 1998](#)
- J. [CDC-90, Federal Advisory Committee Meeting Minutes, December 21, 2000](#)
- K. [CDC-102, CDC/ATSDR Policy on Releasing and Sharing Data, April 16, 2003](#)
- L. Department of Commerce's Commodity Control List
- M. [Department of Defense Military Critical Technology List](#)
- N. [Executive Order 12731, "Principles of Ethical Conduct For Government Officers and Employees"](#)
- O. [Executive Order 12600, Predisclosure Notification Procedures for Confidential Commercial Information](#)
- P. [Executive Order 12958, Classified National Security Information](#)
- Q. [Executive Order 13292, National Security Information](#)
- R. [Export Administration Regulations \(EAR\)](#)
- S. [Freedom of Information Reform Act of 1986 as Amended.](#)
- T. [GSA PBS 3490.1 March 8, 2002, GSA Order Safeguarding Sensitive Unclassified Information \(ADM 1800.3B\)](#)
- U. GSA Instructional Letter CIO IL-99-1, Safeguarding Sensitive Unclassified Information
- V. [GSA Acquisition Manual \(GSAM\) \(ADP P2800.12B\).](#)
- W. [International Traffic in Arms Regulations \(ITAR\)](#)
- X. [National Security Decision Directive \(NSDD\) 298, January 1988, National Operations Security \(OPSEC\) Program](#)
- Y. [Public Law 107-188 Public Health Security and Bioterrorism Preparedness Response Act of 2002](#)
- Z. [Public Law 107-347 E-Government Act of 2002; Federal Information Systems Management Act](#)
- AA. [Public Law 100-235 Computer Security Act of 1987](#)



## Exhibit I

### CDC Common Information Types with Sensitivity Guidance

#### Overview

This document is part of CDC's information and security categorization guidance. It was created to assist the agency and its programs in their efforts to comply with Federal information security management regulations and supporting National Institute of Standards and Technology (NIST) standards. This document outlines categories of commonly used agency information, known as information types. This document also provides guidance on the content and general sensitivity of each information type and, in cases where information may be deemed sensitive, identifies corresponding Freedom of Information Act (FOIA) exemptions.

#### How to Use This Document

The purpose of this document is to provide information owners with a standardized listing of CDC-specific information types and to assist in the identification of potentially sensitive data. The information types described in this guide are applicable across all mission areas and apply to both hardcopy documents and computerized information systems. Typically, hardcopy information is assigned a sensitivity or confidentiality rating that indicates to users how the document must be accessed, stored, and controlled. Information used by computer systems may also be assigned a confidentiality rating but will have additional requirements for integrity and availability. In the case of information systems, these requirements form the security categorization rating for the system and relate directly to the protective controls required for safe and effective operation.

#### Information Sensitivity Ratings at CDC

The majority of information managed by CDC consists of public (non-sensitive) data. However, CDC also handles Sensitive but Unclassified (SBU) information and some National Security (Classified) materials. These designations are fully defined in CDC Classification Policies but are briefly described here for reference. Note: In the event of any discrepancy, CDC Classification Policies should be considered authoritative.

Classified information is information that has been determined, pursuant to Executive Order or law, to require protection against unauthorized disclosure. This information is typically associated only with national security interests and will be marked accordingly. When in doubt regarding the nature of a given data set or system, information owners should refer to NIST SP 800-59, [Guideline for Identifying an Information System as a National Security System](#) and should contact the Chief Information Security Officer (CISO).

Any other information, the unauthorized release of which could cause harm to the agency, its mission, employees, constituents, the public, or the national interest, *and* which meets one or more FOIA exemptions or qualifies for non-disclosure under some other protective statute, should be considered SBU. SBU is the formal designation for information that by law or regulation requires some form of protection but is outside the formal system of classification, as in accordance with Executive Order 12958, as amended.

Information that is identified as neither Classified nor SBU is considered public.

Please note that this guidance applies only to agency public and SBU information. Please refer to [Information Resources Management Policy CDC-05](#) for guidance on classified data.

#### The FOIA Process and Suggested Exemptions



FOIA allows the public to request a wide range of information from Federal agencies. In order to protect sensitive information, FOIA provides nine exemptions that can be used to prevent mandatory release. There are several laws, in addition to FOIA, that may specifically block the disclosure of certain information types. By definition, information that does not qualify under FOIA exemptions or other statutory protections cannot be considered sensitive.

Information owners should consider the applicability of the suggested exemptions defined in the table below when labeling or responding to requests for sensitive data. Please note that only the agency FOIA officer can officially assign exemptions or deny FOIA requests. Even then, some or all information related to a request may be released through departmental appeal or legal proceedings. The suggested exemptions are provided as a guide to allow information owners to better understand and communicate the sensitivity of their information and IT systems. Please consult with the CDC FOIA Officer for a complete listing of FOIA exemptions.

### Understanding the Common Information Types Table

As noted above, the information types and sensitivity guidance provided in this document cover only public and SBU information. The table below is comprised of four columns. Columns 1 and 2, **Information Type** and **Description and Examples**, provide the name and description of each information type. Column 3, **Potentially Sensitive?** indicates the typical sensitivity level of the information type as follows:

- ? **Yes** Information of this type is usually considered to be sensitive. All information types marked as sensitive will have one or more suggested exemptions in Column 4. Information owners should consult CDC policy guidance on the appropriate labeling and information management procedures required for this type of information. Please see Appendix A **References** below for more information.
- ? **Conditional** Information of this type is generally considered non-sensitive, but selected portions of the data may, in fact, require additional protection for example: most portions of a facility plan may be publicly releasable, whereas detailed information regarding certain laboratories may necessitate added protection. In these cases, information owners should identify the sensitive content and consider segregating this data or raising the sensitivity level for all of the information to the level required by the most sensitive parts.
- ? **No** Information of this type is generally considered to be non-sensitive (Public).

Lastly, Column 4, **Potential Exemptions**, provides information on FOIA exemptions and/or other statutes that may potentially be used to protect sensitive information from mandatory disclosure.

### CDC Common Information Types

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Health Information and Mission Support</b>			
Healthcare Information	Covers non-sensitive and non-proprietary information related to medical products, procedures, drugs, and tests.	No	
Public Health Data and Statistics	De-identified health information and/or information of sufficiently broad detail to prevent the identification of specific individuals	No	

	through association or deduction.		
Non-Public Health Data and Statistics (with Personal Identifying Information)	<p>Data obtained from individuals, organizations, or other agencies under an Assurance of Confidentiality that contains either:</p> <ol style="list-style-type: none"> <li>1) Personally identifying information including one or more of the following: name, home address and phone number, social security number, marital status, legitimacy of children, welfare payments, family fights and reputation, medical condition, date of birth, religious affiliation, citizenship data, genealogical history establishing membership in a Native American Tribe, criminal history records (commonly referred to as "rap sheets"), incarceration of United States citizens in foreign prisons, sexual inclinations or associations, and financial status</li> <li>2) Information granular enough to potentially identify an individual through the information given or through association with other available information (small cell size)</li> </ol>	Yes	<p>FOIA Exemption 3: Public Health Service Act ♦ Sections 301 and 308(d): Assurance of Confidentiality</p> <p>Also:</p> <p>Privacy Act ♦ Based on the nature and function of the system in question and the scope of the information request</p> <p>Note: In 1984, Congress explicitly provided that the Privacy Act is not a statute covered under Exemption 3 and therefore cannot be cited under FOIA.</p>
Mission Support	<p>Covers the dissemination and exchange of information between the Federal Government, citizens, and stakeholders in direct support of mission services, public policy, and/or national interest.</p> <p>Includes official public communications, outreach, constituent service, and the general exchange of non-sensitive information.</p>	No	



	Description and Examples	Potentially Sensitive?	Potential Exemptions
--	--------------------------	------------------------	----------------------

Information Type			
Incident Investigation and Response			
Public Emergency Response Management	Covers information regarding agency strategies, capabilities, procedures, and resources for identification, monitoring, and response to public health emergencies, disasters, and/or other crises.	Conditional	
Investigative Activities	<p>Covers information gathered during, and/or related to, ongoing internal and external law enforcement investigations where that information:</p> <ul style="list-style-type: none"> <li>(A) could reasonably be expected to interfere with enforcement proceedings;</li> <li>(B) would deprive a person of a right to a fair trial or an impartial adjudication;</li> <li>(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy;</li> <li>(D) could reasonably be expected to disclose the identity of a confidential source;</li> <li>(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or</li> <li>(F) could reasonably be expected to endanger the life or physical safety of any individual.</li> </ul> <p>In this context ♦ law enforcement ♦ includes criminal, civil and administrative / regulatory proceedings.</p>	Yes	<p>FOIA Exemption 7(A) ♦ While an investigation is pending ♦ other exemptions or Exemption 7 subparts must be used if the information remains sensitive following enforcement procedures</p> <p>Also:</p> <p>FOIA Exemption 2 ♦ Risk of Circumvention</p> <p>FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 ♦ When dealing with events and information related to select agents and toxins and the Strategic National Stockpile.</p>
Strategic National Stockpile	Covers information relating to the locations of US pharmaceutical stockpiles	Yes	<p>FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002</p> <p>Also:</p> <p>FOIA Exemption 2 ♦ Risk of circumvention may be used to protect information regarding specific contents.</p>



Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Select Agents and Bioterrorism</b>			
Select Agents	Covers information about the registration and transfer of Select Agents and Toxins, including the identity and location of specific registered persons.	Yes	FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002  Also:  FOIA Exemption 2 ♦ Risk of circumvention may be used when dealing with safeguards, controls, and/or physical or electronic vulnerability assessments related to select agents.
Bioterrorism Monitoring and Surveillance Activities	Covers information related to the systems, processes, procedures, techniques, and algorithms used to monitor for signs of bio-terrorist activity and events.	Yes	FOIA Exemption 2 ♦ Risk of Circumvention  Also:  FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 ♦ when dealing specifically with Select Agents and Toxins
Bioterrorism Events / Suspected Events and/or Response	Covers ongoing investigative / evidentiary information and other sensitive details surrounding an event or suspected event and response operations.  Note that protection under Exemption 7(A) is lost after enforcement procedures are completed and sensitive information must be protected under other exemptions or other exemption 7 subparts.	Yes	FOIA Exemption 7(A) ♦ while an investigation is pending, other Exemption 7 subparts during and after enforcement procedures are complete.  Also:  FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 ♦ when dealing with Select Agents and Toxins.  FOIA Exemption 4 ♦ If dealing with information that may expose the trade secrets or proprietary information of an entity supplied during the investigation.  FOIA Exemption 6 and/or

			Exemption 3: Public Health Service Act ♦ Section 308 (d): Assurance of Confidentiality ♦ If dealing with personal identifying information (victims, decontamination, follow-up, etc.)
--	--	--	---



Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Third Party Confidential Information</b>			
Third Party Trade Secrets, Confidential, and Proprietary Information	<p>Covers information supplied to the government by a third party that includes ♦ trade secrets ♦ or other privileged or confidential information, such as product manufacturing and design data, business sales statistics, research data, technical designs, currently unannounced and future products, customer and supplier lists, names of consultants and subcontractors, raw research data used to support a pharmaceutical drug's safety and effectiveness, information regarding an unapproved application to market a drug in a different manner, sales and distribution data of a drug manufacturer, profit and loss data, overhead and operating costs, and information on financial condition.</p> <p>For purposes of this exemption, disclosure of the information must either:</p> <ol style="list-style-type: none"> <li>1) impair the government's ability to obtain necessary information in the future, or</li> <li>2) cause substantial harm to the competitive position of the party from whom the information was obtained.</li> </ol>	Yes	<p>FOIA Exemption 4 ♦ Proprietary Information</p> <p>Note: The D.C. circuit resolved that the Trade Secrets Act is not considered a statute under Exemption 3 and therefore cannot be cited under FOIA.</p>
Contractor Technical Proposals	Covers contractor technical proposals where the proposal is not set forth or incorporated by reference into an ensuing government contract.	Yes	FOIA Exemption 3: National Defense Authorization Act ♦ 41 U.S.C. Section 253b(m)
Contractor Business Proposals	Covers contractor business proposals.	Yes	FOIA Exemption 4 ♦ Proprietary Information

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Personnel and Human Resources Information</b>			
General Personnel Management	<p>Covers information associated with the recruitment, management, and development of personnel.</p> <p>Such data includes role descriptions, compensation levels, recruiting efforts, the hiring process, benefits management, expense reimbursement, continuing education, career advancement, training and development plans, etc.</p> <p>This category also includes travel management and personnel logistics, except in conjunction with bioterrorism or other homeland security-related events.</p>	No	
Personal Identifying Information and Privacy Act Systems of Records	<p>Covers information identifiable to a specific individual that would constitute a clearly unwarranted invasion of personal privacy ♦ i.e., home address and phone number, social security number, marital status, legitimacy of children, welfare payments, family fights and reputation, medical condition, date of birth, religious affiliation, citizenship data, genealogical history establishing membership in a Native American Tribe, criminal history records (commonly referred to as "rap sheets"), incarceration of United States citizens in foreign prisons, sexual inclinations or associations, and financial status.</p> <p>Note: Personal information that is <b>not</b> generally protected concerning agency workers include name, title, grade, salary, awards, duty stations, position descriptions, job elements, and performance standards.</p> <p>Note: Foreign nationals are entitled to the same privacy rights under the FOIA as are U.S. citizens.</p>	Yes	<p>FOIA Exemption 6</p> <p>Also:</p> <p>Privacy Act ♦ Based on the nature and function of the system in question and the scope of the information request.</p> <p>Note: In 1984, Congress explicitly provided that the Privacy Act is not a statute covered under Exemption 3 and therefore cannot be cited under FOIA.</p> <p>Records that do not qualify as exempt under FOIA usually cannot be protected under the Privacy Act.</p>
Security Clearance and/or Background Investigations	Covers information resulting from background and security investigations.	Yes	<p>FOIA Exemption 6</p> <p>Also:</p> <p>FOIA Exemption 3: Public Health Security and</p>

			<p>Bioterrorism Preparedness Act of 2002</p> <p>◆ in cases where the investigation is conducted in relation to the possession, handling, or storage of Select Agents and Toxins.</p>
Agency Worker Disclosures	<p>Covers the content of financial disclosures, conflict of interest waivers, and outside activity disclosures sometimes required for Federal employees and contractors.</p> <p>Note: Information concerning high-ranking agency personnel may sometimes still be disclosed.</p>	Yes	<p>FOIA Exemption 3: Ethics in Government Act</p> <p>Note: Consult the agency FOIA Office for information on what is publicly available under the Act.</p>
Misconduct Investigations Concerning Agency Workers	<p>Covers information gathered during investigations of federal employee or contractor misconduct, including the details and results of internal investigations into allegations of impropriety.</p> <p>Note: Information regarding misconduct investigations into the actions of high-ranking federal employees is much more difficult to protect.</p>	Yes	<p>FOIA Exemption 7(A) ◆ while an investigation is pending, must switch to Exemption 6 or other Exemption 7 subparts following closure of the investigation.</p> <p>FOIA Exemption 6</p> <p>Note: In some instances a ◆glomar◆ (neither confirm nor deny) response is appropriate.</p>





Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Facilities Management and Physical Protections</b>			
General Facilities and Equipment Management	<p>Covers information regarding the maintenance, administration, and operation of office buildings, laboratories, environmental controls, machinery, and other capital assets considered possessions of the Federal government.</p> <p>Such information includes space management and planning data, diagrams, floor plans, space and equipment management practices, statistics, operational requirements and usage information, maintenance schedules, resource capabilities, etc.</p>	Conditional	
Detailed Facility Plans, Diagrams, and Blueprints	Covers detailed information regarding agency facilities including blueprints, diagrams, containment / storage areas, and schematics as well as laboratory access, contents, and/or construction information that could aid an attacker by facilitating an intrusion or attack.	Yes	FOIA Exemption 2 ♦ Risk of circumvention
Physical Security Protections and Monitoring	Covers information concerning physical controls and procedures where disclosure could facilitate breach and/or compromise of agency facilities or secure areas. Specific examples include: information about alarm systems, codes, locks, keys, electronic key cards, physical entry systems, cameras, guard rotations and standard operating procedures, environmental controls, and identification badges.	Yes	FOIA Exemption 2 ♦ Risk of circumvention
Internal Emergency Response Management	<p>Covers information related to internal emergency response processes, equipment, and capabilities.</p> <p>Includes emergency responder information, response management and evacuation procedures, containment plans, pre-release public relations information, etc.</p>	Yes	FOIA Exemption 2 ♦ Risk of circumvention

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Agency Management Activities</b>			
Strategic and Operational Planning	<p>Covers information involving the activities of determining strategic direction, identifying and establishing programs and processes to enable change, and allocating resources (capital and labor) among those programs and processes.</p> <p>Includes the budgetary formulation; strategic, capital, and resource planning; budget management and improvement processes.</p>	Conditional	
Program Monitoring, Oversight, Audit, and Evaluation	<p>Covers information used to ensure that the operations and programs of the Federal government and its external business partners comply with applicable laws and regulations, and that may be used to prevent waste, fraud, and abuse.</p> <p>Includes information about monitoring, measurement, evaluation, oversight processes, and findings.</p>	Conditional	
Non-Public Agency Plans, Budgets, and/or Policies (In Development and/or Prior to Approval and Release)	<p>Covers agency working documents and supporting research developed during the decision-making process, including items such as pre-release budgets, draft policies, and strategic plans as well as supporting research materials and recommendations from subject-matter experts or other consultants.</p> <p>Note that selected post-decisional materials may be subject to release unless protected under other exemptions.</p>	Yes	<p>FOIA Exemption 5 ♦ Pre-Decisional / Deliberative</p> <p>Also:</p> <p>FOIA Exemption 2 ♦ Risk of circumvention of controls through release of the material (for example ♦ strategic plans for physical or cyber security may qualify).</p> <p>Other exemptions as allowed based on the specific topic under consideration.</p>
Legal Counsel and Affairs	<p>Covers inter- and intra-agency information concerning legal advice, recommendations, opinions, and materials developed under the ♦attorney-client♦ and ♦attorney work-product♦ privileges.</p>	Yes	FOIA Exemption 5

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Agency Operations</b>			
Workplace Policy Management	Covers information related to the development and dissemination of workplace policies such as dress codes, time reporting requirements, telecommuting, etc.	No	
Records Management and Public Relations	Covers agency information related to records management, administrative (non-mission-related) communications, and public relations.	Conditional	
Financial Management	Covers information related to the aggregate set of accounting practices and procedures that allow for the accurate, efficient, transparent, and effective handling of all government revenues, funding, and expenditures.  Includes financial reporting, budget management, payment and grant processing, collections and receivables processing, and general accounting management functions	Conditional	
Acquisition and Inventory Control	Covers information associated with purchasing, tracking, and the overall management of goods and services.  Includes procurement processes; quality, quantity and location of assets; and the procurement and management of contract services.	Conditional	



Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
<b>Information Technology</b>			
Communications Infrastructure	Covers information related to agency telecommunications systems, networks, and infrastructures.	Conditional	
General Information Management	<p>Covers information related to the information technology resources and processes required to support or enable mission services.</p> <p>Includes policy and standards development, computing environments, architecture, infrastructure, planning, design, development, change management, maintenance, helpdesk, support, and disposal processes.</p>	Conditional	
Authentication Credentials	<p>Covers authentication information and credentials (specifically user IDs, passwords, pin numbers, and digital certificates).</p> <p>Note that system authentication credentials should be designated with at least the same level of sensitivity concern as assigned to the highest rated (most sensitive) information managed by the system.</p>	Yes	FOIA Exemption 2 ♦ Risk of circumvention
Detailed Computer / Network System Configurations and Management Practices	<p>Covers information regarding the details of agency computer systems such that could be used to facilitate circumvention of acceptable use and protective controls.</p> <p>Specific examples include lists of IP addresses, system architecture diagrams, application source code listing, specification documents, procedural and operational processes, storage locations, disposal practices, etc.</p>	Yes	FOIA Exemption 2 ♦ Risk of circumvention
Information Security Protections and Controls	<p>Covers information concerning the security controls, measures, and configuration settings of agency computer systems where disclosure could facilitate circumvention and/or compromise of those systems.</p> <p>Specific examples include: lists of user IDs and passwords, firewall rules, system and network diagrams, specific descriptions of protective controls and/or operational processes (i.e., timing of backups,</p>	Yes	FOIA Exemption 2 ♦ Risk of circumvention

	location of hot site, monitoring practices, etc.), specific identification of sensitive hosts and systems, architecture descriptions, application source code, continuity of operations plan details, and system security plans.		
Vulnerability / Risk Assessments and/or Penetration Test Procedures and Results	<p>Covers information concerning the timing, conduct, participants, processes, tools, results, and derivative reports stemming from vulnerability and risk assessments and/or penetration tests of agency electronic and/or physical systems, facilities, and environments.</p> <p>Includes tests conducted during system Certification and Accreditation (C&amp;A) processes, Office of Inspector General (OIG) audits, annual updates, routine testing and evaluation, and any other assessments as scheduled by agency management.</p>	Yes	FOIA Exemption 2  Risk of circumvention
Continuity of Operations (COOP) and Disaster Recovery (DR) Plans	Covers COOP and DR plan documents as well as detailed information concerning recovery methods, strategies, tools, providers, agreements, priorities, timeframes, and facilities.	Yes	FOIA Exemption 2  Risk of circumvention

**Exhibit 2: Summary Listing of CDC Common Information Types****Health Information and Mission Support**

- ? Healthcare Information
- ? Public Health Data and Statistics
- ? Non-Public Health Data and Statistics (with Personal Identifying Information)
- ? Mission Support

**Incident Investigation and Response**

- ? Public Emergency Response Management
- ? Investigative Activities
- ? Strategic National Stockpile

**Select Agents and Bioterrorism**

- ? Select Agents
- ? Bioterrorism Monitoring and Surveillance Activities
- ? Bioterrorism Events / Suspected Events and/or Response

**Third Party Confidential Information**

- ? Third Party Trade Secrets, Confidential, and Proprietary Information
- ? Contractor Technical Proposals
- ? Contractor Business Proposals

**Personnel and Human Resources Information**

- ? General Personnel Management
- ? Personal Identifying Information and Privacy Act Systems of Records
- ? Security Clearance and/or Background Investigations
- ? Agency Worker Disclosures
- ? Misconduct Investigations Concerning Agency Workers

**Facilities Management and Physical Protections**

- ? General Facilities and Equipment Management
- ? Detailed Facility Plans, Diagrams, and Blueprints
- ? Physical Security Protections and Monitoring
- ? Internal Emergency Response Management

**Agency Management Activities**

- ? Strategic and Operational Planning
- ? Program Monitoring, Oversight, Audit, and Evaluation
- ? Non-Public Agency Plans, Budgets, and/or Policies (In Development and/or Prior to Approval and Release)
- ? Legal Counsel and Affairs

**Agency Operations**

- ? Workplace Policy Management
- ? Records Management and Public Relations
- ? Financial Management
- ? Acquisition and Inventory Control

**Information Technology**

- ? Communications Infrastructure
- ? General Information Management
- ? Authentication Credentials
- ? Detailed Computer / Network System Configurations and Management Practices
- ? Information Security Protections and Controls
- ? Vulnerability / Risk Assessments and/or Penetration Test Procedures and Results
- ? Continuity of Operations and Disaster Recovery Plans



---

[\[1\]](#) References to CDC also apply to the Agency for Toxic Substances and Disease Registry (ATSDR).

Category: Information Security  
Policy #: CDC-IS-2005-02  
Date of Issue: 07/22/2005, Updated 2/22/2006  
Proponents: Office of Security and Emergency Preparedness

## SENSITIVE BUT UNCLASSIFIED INFORMATION

### SECTIONS

- I. [PURPOSE AND SCOPE](#)
- II. [BACKGROUND](#)
- III. [ACRONYMS AND DEFINITIONS](#)
- IV. [POLICY](#)
- V. [RESPONSIBILITIES](#)
- VI. [PROCEDURES](#)
- VII. [REFERENCES](#)
- VIII. [ADDITIONAL RESOURCES](#)

### I. PURPOSE AND SCOPE

The purpose of this issuance is to provide policy and procedures that allow the Centers for Disease Control and Prevention (CDC)<sup>[1]</sup> to accomplish its public health mission while safeguarding data and documents that are sensitive enough to require protection but that may not otherwise be designated as classified information.

This policy applies to all employees, fellows, guest researchers, attached uniformed service members (United States Public Health Service [USPHS] Commissioned Corps, Department of Defense employees, and service members) contractors, subcontractors, or any other individual working at CDC or under the auspices thereof.

### II. BACKGROUND

CDC is required by [OMB Circular A-130, Management of Federal Information Resources](#), to

◆Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.◆

Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable activities may reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions ([National Security Decision Directive Number 298](#)). This policy is intended to minimize this risk.

### III. ACRONYMS AND DEFINITIONS

#### A. For the purposes of this policy, the following acronyms apply:

1. **CC/CO** ♦ coordinating centers and coordinating offices
2. **CISO** ♦ Chief Information Security Officer
3. **DCO** ♦ document control officer
4. **HHS** ♦ Department of Health and Human Services
5. **FOIA** ♦ Freedom of Information Act
6. **ITSO** ♦ Information Technology Services Office
7. **NC** ♦ national center
8. **NSDD** ♦ National Security Decision Directive
9. **OSEP** - Office of Security and Emergency Preparedness
10. **SDT** ♦ HHS Office of Security and Drug Testing
11. **SBU** ♦ sensitive but unclassified

#### B. For the purposes of this policy, the following definitions apply:

##### 1. Document control officer

- a. NC<sup>[2]</sup> and office-level DCO ♦ Employees at the NC or office level who are given responsibility by their NC or office director for the proper maintenance of records related to monitoring, safeguarding, storing, transmitting, and destroying information that is categorized as SBU in compliance with [NSDD-189, National Policy on the Transfer of Scientific, Technical, and Engineering Information](#).
- b. CC/CO DCO ♦ Employees at the CC/CO-level who are given responsibility by their CC/CO director to review decisions made and/or to provide guidance to the NC or office DCO level.
- c. OSEP DCO ♦ When questions of sensitivity arise that cannot be decided at the NC, office, or CC/CO levels, the OSEP DCO shall serve as the final approval authority. The OSEP DCO shall also be responsible for conducting necessary training related to this policy.

##### 2. Electronic media

Electronic media include magnetic tape reels, disk packs, diskettes, compact discs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes, microcassettes, videotapes, and any other device on which data are stored and that normally is removable from the system by the user or operator.

##### 3. Exclusion area

An exclusion area is a security area with barriers that identify the boundaries and encompass the designated space and includes access controls and intrusion detection to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to an exclusion area requires a proximity card, access authorization, and a demonstrated need to know. The CDC♦s current and proposed select agent laboratories are designated as exclusion areas.

##### 4. Export controlled information or material



Export controlled information or material is information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State. This pertains to items controlled by the International Traffic in Arms Regulations or the Department of Commerce and includes items controlled by the Export Administration Regulations. Export controlled information must be controlled as SBU information and marked accordingly.

## 5. **Freedom of Information Act**

The law that requires the release of publicly requested information with several exceptions:

- a. Exemption 1: Information that is currently and properly classified.
- b. Exemption 2: Information that pertains solely to the internal rules and practices of the agency and disclosure of which would allow circumvention of agency regulations.
- c. Exemption 3: Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- d. Exemption 4: Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.
- e. Exemption 5: Intra-agency memoranda that are deliberative in nature. This exemption is appropriate for internal documents that are part of the decision-making process and contain subjective evaluations, opinions, and recommendations.
- f. Exemption 6: Information that, if released, could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- g. Exemption 7: Records or information compiled for law enforcement purposes that:
  - i. could reasonably be expected to interfere with law enforcement proceedings;
  - ii. would deprive a person of a right to a fair trial or impartial adjudication;
  - iii. could reasonably be expected to constitute an unwarranted invasion of personal privacy of others;
  - iv. discloses the identity of a confidential source;
  - v. discloses investigative techniques and procedures; or
  - vi. could reasonably be expected to endanger the life or physical safety of any individual.
- h. Exemption 8: Certain records of agencies responsible for supervision of financial institutions.
- i. Exemption 9: Geological and geophysical information concerning wells.

## 6. **Limited area**

A limited area is a security area residing within the property protection area (see definition of property protection areas) with barriers that identify its boundaries and encompass the designated space. The perimeter of a building often defines the boundaries of a limited area.

It has access controls and intrusion detection in place to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to a limited area requires a proximity card and access authorization.

#### **7. Property protection areas**

Property protection areas are defined by the outermost perimeter of the CDC facility, and this security area is established to protect against damage, destruction, and theft of CDC-owned property. At the Roybal site, the perimeter fence establishes the property protection area; it defines the boundaries of the Roybal Campus and controls personnel and vehicle access.

#### **8. Proprietary Information**

Proprietary information is information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.

#### **9. Sensitive but unclassified**

The **◆sensitive but unclassified◆** designation is applied to unclassified information that may be exempt from mandatory release to the public under FOIA. (For the nine FOIA exemptions, see the FOIA definition in this section.) SBU is the formal designation for information that, by law or regulation, requires some form of protection but is outside the formal system of classification, in accordance with [Executive Order 12958](#), as amended.

#### **10. Special exclusion area**

A special exclusion area is a security area with barriers that identify its boundaries and encompass the designated space. Further, it includes access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to a special exclusion area requires a proximity card, access authorization, demonstrated need to know, and intrusion detection. Personnel authorized for access to these areas are required to hold the appropriate level of security clearance.

### **IV. POLICY**

All CDC employees and otherwise affiliated persons shall protect SBU information by following the procedures contained in this policy document and/or related policies of CDC, HHS, Executive Orders, other Presidential Directives, United States Federal Court rulings, and applicable laws of the United States of America.

### **V. RESPONSIBILITIES**

#### **A. Responsibilities of CDC OSEP Director (or the director◆s designee) with regard to SBU information**

1. Appoint one or more OSEP DCO(s) to implement this policy and procedures.
2. Conduct SBU training.
3. Provide guidance and advice to CC/CO and NC and office DCOs.
4. Form an appeal board, as needed, to render timely judgments concerning appeals to sensitivity determinations.
5. Forward challenges to sensitivity decisions to the SDT.



**B. Responsibilities of CC/CO directors (or their designees) with regard to SBU information**

Each CC/CO director (or the CC/CO director's designee) shall appoint one or more CC/CO DCO(s) to review decisions made at the NC or office DCO level and to provide guidance to NC and office DCOs.

**C. Responsibilities of NC and office directors (or their designees) with regard to SBU information**

Each NC or office director (or the NC or office director's designee) shall appoint one or more NC or office DCO(s) to review all submitted materials; render a sensitivity determination; and maintain records related to monitoring, safeguarding, storing, transmitting, and destroying information that is categorized as SBU in conformance with [NSDD-189, National Policy on the Transfer of Scientific, Technical, and Engineering Information](#).

**D. Responsibilities of NC and office DCO(s) with regard to SBU information**

The NC and office DCO(s) shall review all submitted materials and render a sensitivity determination in accordance with this policy and applicable other laws, orders, rules, and regulations. Sensitivity determinations shall be documented in writing. Files will be maintained in accordance with the [CDC Records Control Schedule](#).

NC- and office-level DCOs are responsible for reviewing and approving information for internal release, Web site content, and to clear policies and procedures for posting on the Intranet.

NC- and office-level DCOs are authorized to make sensitivity determinations ensuring that certain information is not for public release, and that information should be marked as SBU. However, any request for information from the public must be forwarded to the FOIA office for a determination and response.

**E. Responsibilities of CC/CO DCO(s) with regard to SBU information**

The CC/CO DCO(s) shall review decisions made by the NC or office DCO, as necessary, and will provide guidance to the NC or office DCO, as appropriate.

**F. Responsibilities of OSEP DCO(s) with regard to SBU information**

The OSEP DCO(s) shall implement this policy and related procedures; conduct necessary training; and provide guidance and advice to CC/CO and NC or office DCOs. When questions of sensitivity arise that cannot be decided upon at the NC, office, or CC/CO level, the OSEP DCO shall serve as the final decision-making authority.

**G. Responsibilities of supervisors with regard to SBU information**

Supervisors shall ensure that only authorized individuals as identified in this policy have access to SBU information. On an annual basis, and more often if necessary, supervisors shall inform their employees of the need to protect SBU information and of the requirement to have all documents that they create that might contain SBU should be sent to the NC- or office-level DCO(s) for a sensitivity determination. Supervisors shall enforce the procedures of this policy among their employees and within the work spaces for which they are responsible. Supervisors shall report suspected or known violations of this policy or procedures to the CC/CO DCO(s) immediately.

**H. Responsibilities of employees and affiliated persons with regard to SBU information**



Employees and affiliated persons, as provided in Section I of this policy, shall become knowledgeable of this policy and procedures and comply with the requirements established.

#### **I. Responsibilities of CDC FOIA Officer with regard to SBU information**

The CDC FOIA Officer shall provide advice, assistance, policy, and technical guidance on FOIA SBU issues to DCOs and management, as needed. The CDC FOIA Officer will obtain a sensitivity determination prior to a final FOIA decision to release or deny CDC records to the public.

#### **J. Responsibilities of CDC CISO with regard to SBU information**

The CDC CISO shall provide advice, assistance, policy, and technical guidance on information systems security with emphasis on [Federal Information Security and Management Act of 2002](#), and the [Computer Security Act of 1987](#).

### **VI. PROCEDURES**

The following procedures should be followed with regard to SBU:

#### **A. Review and approval of information prior to public release**

The CC/CO and NC- or office-level DCOs are authorized to review and approve information for posting on the CDC Intranet Web site and to make sensitivity determinations to ensure that certain information is not for public release and that the information is marked as SBU.

CC/CO and NC- or office-level DCOs are responsible for establishing submission procedures and making these procedures known to affected personnel.

Marking information SBU does not automatically qualify it for a public release exemption. If a public request for a SBU document is received, the information should be reviewed by the CC/CO DCO to determine if it actually qualifies for exemption. However, only the CDC FOIA Officer is delegated the authority to approve withholding information requested by the public under FOIA.

In reviewing documents, the absence of the SBU or other related marking does not necessarily mean the information should be publicly released. Some types of records (e.g., most human resources and financial information) are not normally marked SBU but may still qualify for withholding under FOIA, unless otherwise authorized for release by the individual. Therefore, all information should be reviewed and approved prior to its public release.

The requirement for a sensitivity review applies equally to hard copy and electronic documents. Electronic documents that require sensitivity review include, but are not limited to, submissions to online publications; documents that are drafted or stored on a publicly accessible home page; and submissions to another Internet site, regardless of site or location.

When any portion of information proposed to be disclosed "might" be covered by a nondisclosure agreement, there must be no steps taken toward public disclosure until written permission from the OSEP DCO is received. This is a lifetime obligation that remains in effect as long as the information remains sensitive.

#### **B. Pre-publication review of Web site content**

Information on the Internet may be intended for a limited audience; however, it actually



becomes available to a world-wide audience. The World Wide Web was not designed with security in mind, and unencrypted information is at high risk of compromise. CDC CISO and ITSO guidelines take into account what security access controls, if any, are in effect for specific sites, the sensitivity of the information, and the target audience to which the information is intended.

Most types of SBU information shall not go on a Web site unless that site is protected by encryption.

Before putting unmarked information on a Web site, the information should receive a sensitivity review by the NC or office DCO and/or the CC/CO DCO to which the information belongs. The CC/CO director or the director's representative may also conduct a review of the information.

CDC sensitivity determinations and classification decisions require that when judgments are made that consideration should be given to the potential consequences of aggregation. The term "sensitive by aggregation" refers to the fact that information on one Web site may seem unimportant, but, when combined with information from other Web sites, it may form a larger and more complete picture than was intended or desired. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that the Web site will be accessed by those seeking information that can be used against CDC.

Personal information ♦ such as addresses; telephone numbers, other than those readily available to the public; social security numbers; dates of birth; names of family members in biographical summaries, etc. ♦ should not be posted on the Internet.

### **C. Sensitivity decision and notification**

If a sensitivity decision is in question after review by the NC- or office-level DCO and the CC/CO DCO, the decision should be referred by the CC/CO DCO to the OSEP DCO via e-mail or inter-office mail. The OSEP DCO shall issue a decision within 15 working days as to the sensitivity of information of a draft document. If a decision cannot be made, or if it is determined that the information should be classified, the document will be sent to either a security review panel at CDC OSEP and/or forwarded to SDT for a sensitivity determination. The originator will be promptly notified as to the status of the document by the OSEP DCO.

### **D. Appeal of sensitivity decision**

Sensitivity determinations may be appealed by a formal written request via e-mail or inter-office mail from the originator through the affected CC/CO director and sent to the Director of OSEP for a final determination.

### **E. Categories of SBU Information**

Sensitive information consists of any information exempted from FOIA and includes, but is not limited to, information related to personnel, security, and select agents.

Examples include, but are not limited to:

**1. Personnel**

General personnel information such as evaluation and performance data; security information, including background investigation results and adjudication, and infractions/incident reports; personal information, when associated with an individual's work on topics where security is involved (e.g., names and details of those working with select agents, classified data, counterintelligence) or with those individuals who are authorized to have a level of access beyond the average CDC employee/contractor/visitor.

**2. Security**

Facility blueprints and other detailed facility information; databases associated with the physical security system; vulnerabilities of such facilities or sensitive information; network security information; security procedures; access codes (combinations or passwords); badge design information; security audit results; physical security performance test results; results of response force exercises; incident reports and disciplinary actions; response force capabilities; and security plans.

**3. Select agents**

Databases and lab records associated with the select agent program including, but not limited to, inventory databases and chain of custody records; select agent transfer records; documentation associated with an experiment resulting in an unexpected result banned by [9 CFR 121.10](#); and information deemed too sensitive for public release by a review and approval panel.

**F. SBU mandatory release exemptions under FOIA**

Information in either electronic or hard copy form determined to be SBU must fall within one or more of the nine FOIA exemption categories identified in Section II. B. 5. to be exempt from mandatory release to the public.

**G. SBU personnel access requirements**

United States citizen direct-hire supervisory employees are responsible for access, dissemination, and release of SBU material. Employees will limit access to protect SBU information from unintended public disclosure.

Employees may circulate SBU materials to others, including non-United States citizens, to carry out an official United States Government function, if not otherwise prohibited by law, regulation, or interagency agreement.

## **H. SBU safeguarding and storage requirements**

### **1. Protection of SBU information while in use**

Reasonable precautions should be taken to prevent access to sensitive information by persons who do not require the information to perform their jobs (e.g., sensitive documents should not be read in a public place or taken home).

### **2. Storage rules for SBU information**

Sensitive information, both in hard copy and electronic form, should be physically protected and should be stored in limited areas. Exclusion areas and special exclusion areas are also acceptable storage locations, but high containment laboratories should only be used as storage areas for sensitive information when absolutely necessary. Storing sensitive information in a property protection area or a public area is only acceptable if additional protections are taken to increase protection to a level comparable to that in a limited area.

All sensitive information existing in hard copy should be stored within a locked container in a limited or exclusion area, an access controlled electronic environment, or under the physical control of an authorized individual. On occasions when an individual is traveling within the United States and limited or exclusion areas are not available, a locked container within a locked room will suffice (e.g., locked briefcase or suitcase within a locked hotel room or vehicle). Sensitive information should not be taken outside the United States.

Information handled electronically and transmitted over the network is at a higher risk of being released or altered. Sensitive information stored on the CDC network should be protected at a level that can ensure that only those who are authorized to view the information are allowed access (e.g., machine-generated passwords, encryption). The CDC network systems should maintain a high level of electronic protection (e.g., firewalls, intrusion detection, defense-in-depth, isolation of sensitive information, good practices network administration) to ensure the integrity of sensitive information and to prevent unauthorized access into these systems. Regular review of the protection methods used and system auditing are also critical to maintain protection of these systems.

The physical elements of the network systems that store and transmit sensitive information or that have direct access to sensitive information should be secured within a limited area or exclusion area. The more central the information resource is (e.g., a network or security system control room), the higher the level of access control that should be applied.

## **I. SBU marking requirements**

Information that has been determined to be SBU should be designated as SBU with the following appropriate markings and labels:

## 1. Documents

Documents containing sensitive information should be covered with a **Sensitive But Unclassified** cover page, and the outside of the back cover should be marked **Sensitive But Unclassified**.

Internal pages of the document should be marked **Sensitive But Unclassified** at the top and bottom of each page in letters clearly distinguishable from the text. The acronym SBU may be used when space does not permit spelling out **Sensitive But Unclassified**.

The first page should contain the following statement at the lower left hand corner and should be completed with the applicable FOIA exemption number(s):

**Sensitive But Unclassified (SBU)**

This document contains information that may be exempt from public release under the Freedom of Information Act (FOIA) (5 U.S.C. 552), exemption(s) \_\_\_\_\_ apply. Approval by the Centers for Disease Control and Prevention Document Control Officer, Office of Security and Emergency Preparedness, and the CDC FOIA Officer, prior to public release via the FOIA Office is required.

## 2. Electronic media

Electronic media containing sensitive information should be labeled **Sensitive But Unclassified**. The label should be plainly visible and should be applied in a way that does not interfere with the drive mechanism. The outer covering for any of the above removable storage media should also be marked **Sensitive But Unclassified**.

Videotapes should also contain **Sensitive But Unclassified** at the beginning and end of the played video, if possible. Audio cassettes, if possible, should contain an audible statement at the beginning and end of the played portion that informs the listener that the tape contains SBU information.

## 3. Blueprints, engineering drawings, charts, and maps

Blueprints, engineering drawings, charts, and maps containing sensitive information should be marked **Sensitive But Unclassified - Building Information** or "SBU-BI" at the top and bottom of each page. If the blueprints, drawings, charts, or maps are large enough that they are likely to be rolled or folded, **Sensitive But Unclassified - Building Information** should be placed so that the marking is visible when the item is rolled or folded.

## 4. Photographs and negatives

Photographs containing sensitive information should be marked **Sensitive But Unclassified** on the face, if possible. If this cannot be done, the marking should be placed on the reverse side. Negatives, positives, or other film containing sensitive information should be marked **Sensitive But Unclassified** on the film itself, if possible; otherwise, it should be protected inside a marked container.

## J. Reproduction of SBU information

SBU documents may be reproduced without the permission of the originator to the extent



necessary to carry out official CDC activities. Copies should be protected in the same manner as originals. In the event of a copy machine malfunction, the copy machine should be cleared and all paper paths checked for papers containing sensitive information.

## **K. SBU transfer requirements**

### **1. Communicating sensitive information**

Sensitive information may be communicated in the following ways:

From person to person in direct contact with one another; over a land-line telephone; via first class, priority, or overnight mail; via fax machine; via e-mail to and from CDC e-mail addresses that reside completely within the CDC network ([...][@cdc.gov](mailto:cdc.gov)); via e-mail to and/or from an e-mail address outside of the CDC network, provided that the sensitive data is encrypted and authenticated.

### **2. Discussing sensitive information via telephone or video conference**

Although sensitive information may be discussed on landline telephones, sensitive information should not be discussed on cellular phones. Sensitive information should not be transmitted via open network communication channels, including online video conferencing unless such a conference is held on a restricted network.

### **3. Mailing of sensitive information**

Transmission of sensitive information should be done in a manner that informs those with a need-to-know of the level of sensitivity while not advertising the fact to the general public. It is also important to use a reliable means of shipping. These considerations help to avoid unauthorized disclosure or dissemination of sensitive information.

### **4. Internal mail**

Before transmitting sensitive information through the CDC internal mail, the information should have appropriate markings and cover sheet and should be placed in a SBU envelope.

### **5. External mail**

Sensitive information sent outside CDC premises should be transmitted via first class mail, priority, or overnight mail. The outer wrapping should not be marked in a manner that would reveal the contents of the envelope or package to unauthorized personnel.

## 6. Faxing of sensitive but unclassified Information

Prior to faxing sensitive information, the sender should confirm that an authorized person will be present to accept the transmittal at the receiving end, or the sender should verify that the receiving facility is protected in a manner sufficient to preclude unauthorized access to the transmitted material.

## 7. Electronic transmission

Sensitive information should be encrypted and authenticated if it is sent from the CDC network to an unsecured (non-CDC) network. Sensitive information should never be communicated over wireless technologies, such as cellular or cordless telephones or wireless data devices (e.g., BlackBerry devices).

## L. SBU disposal and destruction requirements and methods

Sensitive information should be destroyed by shredding or burning; paper containing sensitive information should not be recycled.

Deleting, erasing, or formatting will not sufficiently remove sensitive information from electronic storage formats. Instead, files should be removed by using multiple passes (10 times minimum) of a hard drive wiping program. Electronic or removable media should be physically damaged to the point of inoperability, via shredding, degaussing, melting, or other such methods before disposal.

## M. Enforcement

A violation of this policy may be cause for punitive administrative action, including termination of employment, dismissal, or discharge from USPHS Commissioned Corps. Further civil and criminal prosecution may be sought under one or more of the laws codified in the [United States Code of Federal Regulations](#).

## N. Implementation

Marking requirements identified in this policy apply to documents produced after this policy's implementation date. However, all items, regardless of when they were produced, are subject to the remaining provisions of this policy effective upon the date of this policy's implementation.

## VII. REFERENCES

- A. [CDC Freedom of Information Policy](#). March 19, 2002.
- B. [CDC Records Control Schedule](#). May 15, 1998.
- C. [Computer Security Act of 1987](#), Public Law 100-235 (H.R. 145). January 8, 1988.
- D. [Executive Order 12958, National Security Information](#). April 17, 1995.
- E. [Export Administration Regulations](#). January 27, 2006.
- F. [Federal Information Security Management Act of 2002](#). December 2002.
- G. [Freedom of Information Act](#). September 18, 1996.
- H. [International Traffic in Arms Regulations](#). April 1, 1992.
- I. [National Institute of Standards and Technology: Computer Security](#). July 2003.
- J. [NSDD-189, National Policy on the Transfer of Scientific, Technical, and Engineering Information](#). September 21, 1985.
- K. [United States Code of Federal Regulations \(1996-present\)](#). February 1, 2006.

## VIII. ADDITIONAL RESOURCES

- A. [Arms Export Control Act](#). 1994.
- B. [CDC-IR-2002-06, Protection of Information Resources](#). CDC, April 2002.
- C. [CDC-IR-2002-03, Classified Material](#). CDC, April 2002.
- D. [CDC-IS-2005-03, Use of CDC Information Technology Resources](#). CDC, August 2005.
- E. [CDC-AM-2004-02, Procurement Integrity Restrictions](#). CDC, February 2004.
- F. [CDC-GA-2005-06, Clearance Of Information Products Distributed Outside CDC for Public Use](#). CDC, July 2005.
- G. [CDC-GA-2000-01, Privacy Act](#). CDC, November 2000.
- H. [CDC-GA-2002-02, Freedom of Information Act](#). CDC, March 2002.
- I. [CDC-GA-1998-01, Export Controls for Biological, Chemical, and Related Technical Data and Equipment](#). CDC, June 1998.
- J. [CDC-GA-2000-02, Federal Advisory Committee Meeting Minutes](#). CDC, December 2000.
- K. [CDC-GA-2005-14, CDC/ATSDR Policy on Releasing and Sharing Data](#). CDC, September 2005.

---

<sup>[1]</sup> References to CDC also apply to the Agency for Toxic Substances and Disease Registry (ATSDR).

<sup>[2]</sup> For ease of reference within policy documents, **NC** will refer collectively to CDC's national centers, institute, the National Immunization Program, the Office of Genomics and Disease Prevention, and the Agency for Toxic Substances and Disease Registry (an independent Health and Human Services Agency that is led by the CDC director and for which CDC provides administrative services).



## CONTROLLED UNCLASSIFIED INFORMATION

### SECTIONS

1. [PURPOSE AND SCOPE](#)
2. [BACKGROUND](#)
3. [POLICY](#)
4. [RESPONSIBILITIES](#)
5. [REFERENCES](#)
6. [ADDITIONAL RESOURCES](#)
7. [ACRONYMS AND DEFINITIONS](#)

### 1. PURPOSE AND SCOPE

These procedures allow CDC to accomplish its public health mission while safeguarding data and documents that are sensitive enough to require protection from unauthorized public disclosure, but that may not otherwise be designated as classified information.

This policy applies to all employees, fellows, guest researchers, attached uniformed service members, United States Public Health Service (USPHS) Commissioned Corps, Department of Defense employees and service members, contractors, subcontractors, or any other individual working at CDC or under the auspices thereof.

### 2. BACKGROUND

CDC is required by [OMB Circular A-130, Management of Federal Information Resources](#) to:

“Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.”

Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable activities may reveal the existence of, and sometimes details about, sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions ([National Security Decision Directive \[NSDD\] Number 298](#)). This policy is intended to minimize this risk.

### 3. POLICY

All CDC employees and otherwise affiliated persons shall protect CUI by following the procedures contained in this policy document and related policies of CDC, HHS, and associated Executive Orders.

---

<sup>1</sup> Updated in accordance with White House Memorandum of May 7, 2008 to standardize practices and improve sharing of sensitive information.



CUI consists of any information that under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. CDC organizations may originate or handle sensitive information that should be designated CUI and safeguarded from unauthorized disclosure. CUI at CDC includes, but is not limited to, information related to CDC security, sensitive facilities information, the national stockpile inventory, and select agent information.

## **A. Categories of CUI**

All CDC CUI shall merit one of two levels of safeguarding measures, standard or enhanced.

At the “controlled standard” level the required safeguards are limited to measures that are believed to be practicable for all authorized recipients of CUI to enable rapid, efficient and affordable sharing within the agency and among agency partners and within the Information Sharing Environment (ISE).

At the “controlled enhanced” level more stringent safeguarding measures are required due to the particularly sensitive nature of the information. All controlled enhanced CUI shall be marked to clearly indicate that enhanced safeguards are required and that use of specified dissemination, i.e. specifying the offices or individuals to receive that information shall be utilized.

Until further notice all originators of CUI requiring controlled enhanced safeguarding will require a statement of non-disclosure by authorized recipients. Please contact the OSEP Document Control Officer (DCO) for assistance with CUI requiring enhanced safeguarding and specified dissemination. Once national marking and dissemination guidance from the Executive Agent is received, the CDC CUI Policy will be updated to reflect that guidance.

CUI examples include, but are not limited to:

### **(1) Security**

Facility blueprints and other detailed facility information; databases associated with the physical security system; vulnerabilities of such facilities or sensitive information; network security information; security procedures; access codes (combinations or passwords); badge design information; security audit results; physical security performance test results; results of response force exercises; incident reports and disciplinary actions; response force capabilities; and security plans.

### **(2) National Stockpile Inventory**

Specific information about stockpile inventory, specific location information and location information that associates specific inventory; security procedures or protocols specific to stockpile inventory, logistics or material movements and procedures related to those movements and vendor-related information that identifies commercial acquisition of stockpile inventory.

### **(3) Select agents**

Databases and lab records associated with the select agent program including, but not limited to, inventory databases and chain of custody records; select agent transfer records; documentation associated with an experiment resulting in an unexpected result banned by [7 CFR Part 331](#) and [9 CFR Part 121](#) and information deemed too sensitive for public release by a review and approval panel.

## **B. Procedures**

The following procedures should be followed with regard to CUI.

### **(1) Review and approval of information prior to public release**

Public requests for CUI documents must be reviewed by the CDC FOIA Officer. The requirement for a sensitivity review applies equally to hard copy and electronic documents. Electronic documents that require sensitivity review include, but are not limited to, submissions to online publications; documents that are drafted or stored on a publicly accessible home page; and submissions to another Internet site, regardless of site or location.

### **(2) Pre-publication review of Web site content**

Before putting unmarked information on a website, the information should receive a sensitivity review by the NC or office DCO and/or the CC/CO DCO to which the information belongs. The organization's director or representative may also conduct a review of the information.

CDC sensitivity determinations and classification decisions require that when judgments are made that consideration should be given to the potential consequences of aggregation. The term "sensitive by aggregation" refers to the fact that information on one website may seem unimportant, but, when combined with information from other websites, it may form a larger and more complete picture than was intended or desired. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that the website will be accessed by those seeking information that can be used against CDC.

CUI may not be posted to websites that are publicly available or that limit access only by domain/IP restriction. Encryption must be implemented in accordance with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) which requires basic encryption and authentication standards to include use of a username and a password. Further guidance may be obtained from the OSEP DCO.

Personal information – such as addresses; telephone numbers, other than those readily available to the public; social security numbers; dates of birth; names of family members in biographical summaries, etc. – should not be posted on the Internet.

### **(3) Sensitivity decision and notification**

If a sensitivity decision is in question after review by the NC- or office-level DCO and the CC/CO DCO, the decision should be referred by the CC/CO DCO to the OSEP DCO via e-mail or inter-office mail. The OSEP DCO shall issue a decision within 15 working days as to the sensitivity of information of a draft document. If a decision cannot be made, or if it is determined that the information should be classified, the document will be sent to either a security review panel at CDC OSEP and/or forwarded to SDT for a sensitivity determination. The originator will be promptly notified as to the status of the document by the OSEP DCO.

### **(4) Appeal of sensitivity decision**

Sensitivity determinations may be appealed by a formal written request via e-mail or inter-office mail from the originator through the affected CC/CO director and sent to the Director of OSEP for a final determination.

### **(5) CUI release exemptions under FOIA**

Information in either electronic or hard copy form determined to be CUI may fall within one or more of the nine FOIA exemption categories.

CUI designations may inform but do not control the decision of whether to disclose or release the information to the public in response to a request made pursuant to FOIA. Those decisions are made through the CDC FOIA Office.

### **(6) CUI personnel access requirements**

United States citizen supervisory employees are responsible for access, dissemination, and release of CUI material. Employees will limit access to protect CUI from unintended public disclosure.

Employees may circulate CUI materials to others, including non-United States citizens, to carry out an official United States Government function, if not otherwise prohibited by law, regulation, or interagency agreement.

### **(7) CUI safeguarding and storage requirements**

#### **Protection of CUI while in use**

Reasonable precautions should be taken to prevent access to CUI by persons who do not require the information to perform their jobs (e.g., sensitive documents should not be read in a public place or other places where there is risk of unwanted third party access.)

#### **Storage rules for CUI**

CUI, both in hard copy and electronic form, should be physically protected and should be stored in limited areas. Exclusion areas and special exclusion areas are also acceptable storage locations, but high containment laboratories should only be used as storage areas for sensitive information when absolutely necessary. Storing

CUI in a property protection area or a public area is only acceptable if additional protections are taken to increase protection to a level comparable to that in a limited area. These protections should be in accordance with FIPS 140-2.

All CUI existing in hard copy should be stored within a locked container in a limited or exclusion area, an access controlled electronic environment, or under the physical control of an authorized individual. On occasions when an individual is traveling within the United States and limited or exclusion areas are not available, a locked container within a locked room will suffice (e.g., locked briefcase or suitcase within a locked hotel room or vehicle). CUI should not be taken outside the United States.

Electronic storage must be controlled according to the standards set by the FIPS 140-2 Security Level 1 and the standards maintained by the CDC and HHS information networks. Storage on removable electronic media must be protected by an electronic barrier of encryption set to these standards. CUI should not be stored on personally-owned wireless media devices. Further guidance on electronic storage from the Executive Agent for CUI and CUI requiring controlled enhanced safeguarding will be forthcoming.

#### **(8) CUI marking requirements**

Information that has been determined to be CUI should be designated as CUI with the following appropriate markings and labels:

#### **(9) Documents**

Until specific marking guidance from the Executive Agent for CUI and CUI requiring controlled enhanced safeguarding is available documents containing CUI should be covered with a cover page. The cover page should be marked as indicated below; the outside of the back cover should be marked Sensitive But Unclassified Information (SBU)."

Internal pages of the document should be marked "Sensitive But Unclassified Information (SBU)" at the top and bottom of each page in letters clearly distinguishable from the text. The acronym SBU may be used when space does not permit spelling out "Sensitive But Unclassified Information".

The cover page should contain the following statement at the lower left hand corner:

"Sensitive But Unclassified Information":

This document contains information that requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Approval by the Centers for Disease Control and Prevention Document Control Officer, Office of Security and Emergency Preparedness, and the CDC FOIA Officer, prior to public release via the FOIA Office is required."

One of the following statements about safeguarding and dissemination controls should follow:



- (a) "Standard Dissemination" meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure and dissemination is permitted to the extent that it is reasonably believed would further the execution of an official purpose,
- (b) "Specified Dissemination required to prevent inadvertent or unauthorized disclosure" to require more stringent safeguarding measures than those normally required since the inadvertent or unauthorized disclosure would risk substantial harm and provide additional instructions on what dissemination is permitted.

Contact the OSEP DCO for assistance with specifying dissemination for CUI with controlled enhanced safeguarding measures and for development of a statement of non-disclosure for CUI recipients.

#### **(10) Electronic media**

Electronic media containing CUI should be labeled "Sensitive But Unclassified Information" and include a dissemination statement as outlined above. The label should be plainly visible and should be applied in a way that does not interfere with the drive mechanism. The outer covering for any of the above removable storage media should also be marked "Sensitive But Unclassified Information".

Videotapes should also contain "Sensitive But Unclassified Information" and include a dissemination statement at the beginning and end of the played video, if possible. Audio cassettes, if possible, should contain an audible statement at the beginning and end of the played portion that informs the listener that the tape contains CUI.

#### **(11) Blueprints, engineering drawings, charts, and maps**

Blueprints, engineering drawings, charts, and maps containing sensitive facilities information should be marked "Sensitive But Unclassified Information: Specified Dissemination" at the top and bottom of each page. If the blueprints, drawings, charts, or maps are large enough that they are likely to be rolled or folded, "Sensitive But Unclassified Information: Specified Dissemination" should be placed so that the marking is visible when the item is rolled or folded. Where possible, a cover sheet with the following statement should be included: "Sensitive But Unclassified Information: Specified Dissemination required to prevent inadvertent or unauthorized disclosure."

#### **(12) Photographs and negatives**

Photographs containing sensitive information should be marked "Sensitive But Unclassified Information" and a dissemination statement on the face, if possible. If this cannot be done, the marking should be placed on the reverse side. Negatives, positives, or other film containing sensitive information should be marked "Sensitive But Unclassified Information" on the film itself, if possible; otherwise, it should be protected inside a marked container.

### **(13) Reproduction of CUI**

CUI documents may be reproduced without the permission of the originator to the extent necessary to carry out official CDC activities. Copies should be protected in the same manner as originals. In the event of a copy machine malfunction, the copy machine should be cleared and all paper paths checked for papers containing sensitive information.

### **(14) CUI transfer requirements**

#### **(a) Communicating sensitive information**

Until further guidance regarding specific safeguards for communication CUI is made available from the Executive Agent, CUI may be communicated in the following ways:

- From person to person in direct contact with one another; over a land-line telephone; via first class, priority, or overnight mail; via fax machine; via e-mail to and from CDC e-mail addresses that reside completely within the CDC network ([...]@cdc.gov)
- Via e-mail to and/or from an e-mail address outside of the CDC network, provided that the sensitive data is encrypted and authenticated.

#### **(b) Discussing CUI via telephone or video conference**

Although CUI may be discussed on landline telephones, sensitive information should not be discussed on cellular phones. CUI should not be transmitted via open network communication channels, including online video conferencing unless such a conference is held on an encrypted network.

#### **(c) Mailing of CUI**

Transmission of CUI should be done in a manner that informs the CUI recipient of the information's sensitivity while not advertising the fact to the general public. It is also important to use a reliable means of shipping. These considerations help to avoid unauthorized disclosure or dissemination of CUI.

#### **(d) Internal mail**

Before transmitting sensitive information through the CDC internal mail, the information should have appropriate CUI markings and cover sheet and should be placed in an opaque-envelope.

#### **(e) External mail**

CUI sent outside CDC premises should be transmitted via first class mail, priority, or overnight mail. The outer wrapping should not be marked in a manner that would reveal the contents of the envelope or package to unauthorized personnel. All CUI requiring controlled enhanced safeguarding should be enclosed in a second opaque envelope or wrapping or locked opaque container.

#### **(f) Faxing of CUI**

Prior to faxing CUI, the sender should confirm that an authorized person will be present to accept the transmittal at the receiving end, or the sender should verify that the receiving facility is protected in a manner sufficient to preclude unauthorized access to the transmitted material.

#### **(g) Electronic transmission**

CUI should be encrypted and authenticated if it is sent from the CDC network to an unsecured (non-CDC) network. CUI should only be transmitted on secure, encrypted wireless devices to known CUI recipients that conform to the electronic barrier standards set forth in FIPS 140-2. CUI should not be communicated via personally-owned wireless technologies. Until further guidance from the Executive Agent becomes available, CUI requiring enhanced safeguarding measures will not be communicated via wireless data devices such as blackberries.

### **(15) CUI disposal and destruction requirements and methods**

CUI should be destroyed by shredding or burning. Paper containing sensitive information should not be recycled.

Deleting, erasing, or formatting will not sufficiently remove sensitive information from electronic storage formats. Instead, files should be removed by using multiple passes (10 times minimum) of a hard drive wiping program. Electronic or removable media should be physically damaged to the point of inoperability, via shredding, degaussing, melting, or other such methods before disposal.

### **(16) Enforcement**

A violation of this policy may be cause for punitive administrative action, including termination of employment, dismissal, or discharge from USPHS Commissioned Corps. Further civil and criminal prosecution may be sought under one or more of the laws codified in the [United States Code of Federal Regulations](#).

### **(17) Implementation**

Procedures identified in this interim policy apply to documents produced until such time as final guidance from the Executive Agent is made available. Legacy markings under the previous version of the CDC SBU Policy shall be utilized until that final guidance is received. However, all items, regardless of when they were produced, are subject to the safeguarding provisions of this policy which have been effective since 7/22/2005.

## **4. RESPONSIBILITIES**

### **A. Responsibilities of CDC Office of Security and Emergency Preparedness Director (or the director's designee) with regard to CUI**

- Appoint one or more OSEP document control officers to implement this policy



- Conduct CUI training
- Provide guidance and advice to coordinating center/coordinating office (CC/CO) and national center (NC)<sup>2</sup> and office DCOs
- Form an appeal board, as needed, to render timely judgments concerning appeals to sensitivity determinations
- Forward challenges to sensitivity decisions to the HHS Office of Security and Drug Testing (SDT)

**B. Responsibilities of NC and office directors (or their designees) with regard to CUI**

- Appoint one or more DCO(s) as required to implement this policy
- Review all submitted materials
- Render a sensitivity determination in accordance with this policy and applicable regulations and laws
- Document sensitivity determinations in writing
- Maintained files in accordance with the [CDC Records Control Schedule](#)
- Reviewing and approving information for internal release, website content, and clearing policies and procedures for posting on the Intranet
- Make sensitivity determinations to safeguard CUI information and prevent unintentional or unauthorized public release. However, any request for information from the public must be forwarded to the Freedom of Information Act (FOIA) office for a determination and response.

**C. Responsibilities of CC/CO DCO(s) with regard to CUI**

- Review decisions made by the NC or office DCO, as necessary
- Provide guidance to the NC or office DCO, as appropriate

**D. Responsibilities of OSEP DCO(s) with regard to CUI**

- Implement this policy and related procedures
- Conduct necessary training
- Provide guidance and advice to CC/CO and NC or office DCOs
- Render decisions when questions of sensitivity arise that cannot be decided upon at the NC, office, or CC/CO level
- Serve as the final sensitivity decision-making authority subject to the appeals process in accordance with this policy

---

<sup>2</sup> For ease of reference within policy documents, “national center” will refer collectively to CDC’s national centers, institute, and the Agency for Toxic Substances and Disease Registry (an independent Health and Human Services agency that is led by the CDC director and for which CDC provides administrative services).



#### **E. Responsibilities of supervisors with regard to CUI**

- Ensure that only authorized individuals, as identified in this policy, have access to CUI
- Annually or more often if necessary, inform their employees of the need to protect CUI and of the requirement to have all documents they create that might contain CUI sent to the NC or office-level DCO(s) for a sensitivity determination
- Enforce the procedures of this policy among their employees and within the work spaces for which they are responsible
- Report suspected or known violations of this policy to the CC/CO DCO(s) immediately

#### **F. Responsibilities of employees and affiliated persons with regard to CUI**

Employees and affiliated persons, as provided in Section 1 of this policy, shall become knowledgeable of this policy and procedures and comply with the requirements established.

#### **G. Responsibilities of CDC FOIA Officer with regard to CUI**

- Provide advice, assistance, policy, and technical guidance on FOIA issues to DCOs and management, as needed
- Obtain a sensitivity determination from the appropriate DCO prior to rendering a final FOIA decision to release or deny CDC records to the public
- Make the final decision regarding whether to release information to the public.

#### **H. Responsibilities of CDC Chief Information Security Officer (CISO) with regard to CUI**

The CDC CISO shall provide advice, assistance, policy, and technical guidance on information systems security with emphasis on Federal Information Security and Management Act of 2002, and the [Computer Security Act of 1987](#).

### **5. REFERENCES**

[CDC Freedom of Information Policy](#). March 19, 2002.  
[CDC Records Control Schedule](#). May 15, 1998.  
[Computer Security Act of 1987](#), Public Law 100-235 (H.R. 145). January 8, 1988.  
[Executive Order 12958, National Security Information](#). April 17, 1995.  
[Export Administration Regulations](#). January 27, 2006.  
[Federal Information Security Management Act of 2002](#). December 2002.  
[Freedom of Information Act](#). September 18, 1996.  
[International Traffic in Arms Regulations](#). April 1, 1992.  
[National Institute of Standards and Technology: Computer Security](#). July 2003.  
[NSDD-189, National Policy on the Transfer of Scientific, Technical, and Engineering Information](#). September 21, 1985.  
[United States Code of Federal Regulations \(1996-present\)](#). February 1, 2006.  
[White House Memorandum, Designation and Sharing of Controlled Unclassified Information \(CUI\)](#). May 7, 2008.

## 6. ADDITIONAL RESOURCES

Arms Export Control Act. 1994.

CDC-IR-2002-06, Protection of Information Resources. CDC, April 2002.

CDC-IR-2002-03, Classified Material. CDC, April 2002.

CDC-IS-2005-03, Use of CDC Information Technology Resources. CDC, August 2005.

CDC-AM-2004-02, Procurement Integrity Restrictions. CDC, February 2004.

CDC-GA-2005-06, Clearance Of Information Products Distributed Outside CDC for Public Use. CDC, July 2005.

CDC-GA-2000-01, Privacy Act. CDC, November 2000.

CDC-GA-2002-02, Freedom of Information Act. CDC, March 2002.

CDC-GA-1998-01, Export Controls for Biological, Chemical, and Related Technical Data and Equipment. CDC, June 1998.

CDC-GA-2000-02, Federal Advisory Committee Meeting Minutes. CDC, December 2000.

CDC-GA-2005-14, CDC/ATSDR Policy on Releasing and Sharing Data. CDC, September 2005.

## 7. ACRONYMS AND DEFINITIONS

### A. For the purposes of this policy, the following acronyms apply:

**CC/CO** – coordinating centers and coordinating offices

**CFR** – Code of Federal Regulations

**CISO** – Chief Information Security Officer

**CUI** – Controlled Unclassified Information

**DCO** – document control officer

**HHS** – Department of Health and Human Services

**FOIA** – Freedom of Information Act

**ISE** – Information Sharing Environment

**ITSO** – Information Technology Services Office

**NARA** – National Archives and Records Administration

**NC** – national center

**NSDD** – National Security Decision Directive

**OSEP** - Office of Security and Emergency Preparedness

**SDT** – HHS Office of Security and Drug Testing

### B. For the purposes of this policy, the following definitions apply:

#### **Controlled Unclassified Information**

The CUI designation refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces “Sensitive But Unclassified (SBU).” However, legacy markings of “SBU” will be retained until future guidance from the Executive Agent is promulgated.



## **Document Control Officer**

Employees through-out CDC who are given responsibility by their organization director for the proper maintenance of records related to monitoring, safeguarding, storing, transmitting, and destroying information that is categorized as CUI in compliance with NSDD-189, National Policy on the Transfer of Scientific, Technical, and Engineering Information.

## **Electronic media**

Electronic media include magnetic tape reels, disk packs, diskettes, compact discs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes, microcassettes, videotapes, and any other device on which data are stored and that normally is removable from the system by the user or operator.

## **Exclusion area**

An exclusion area is a security area with barriers that identify the boundaries and encompass the designated space and includes access controls and intrusion detection to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to an exclusion area requires a proximity card, access authorization, and a demonstrated need to know. CDC's current and proposed select agent laboratories are designated as exclusion areas.

## **Export controlled information or material**

Export controlled information or material is information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State. This pertains to items controlled by the International Traffic in Arms Regulations or the Department of Commerce and includes items controlled by the Export Administration Regulations. Export controlled information must be controlled as CUI and marked accordingly.

## **Limited area**

A limited area is a security area residing within the property protection area (see definition of property protection areas) with barriers that identify its boundaries and encompass the designated space. The perimeter of a building often defines the boundaries of a limited area. It has access controls and intrusion detection in place to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to a limited area requires a proximity card and access authorization.

## **Property protection areas**

Property protection areas are defined by the outermost perimeter of the CDC facility, and this security area is established to protect against damage, destruction, and theft of CDC-owned property. At the Roybal site, the perimeter fence establishes the property protection area; it defines the boundaries of the Roybal Campus and controls personnel and vehicle access.

**Proprietary Information**

Proprietary information is information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.

**Special exclusion area**

A special exclusion area is a security area with barriers that identify its boundaries and encompass the designated space. Further, it includes access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to a special exclusion area requires a proximity card, access authorization, demonstrated need to know, and intrusion detection. Personnel authorized for access to these areas are required to hold the appropriate level of security clearance.



## **CLASSIFIED MATERIAL**

<b>Sections:</b>	<b>I. <u>POLICY</u></b>
	<b>II. <u>PURPOSE</u></b>
	<b>III. <u>DEFINITION OF CLASSIFIED MATERIAL</u></b>
	<b>IV. <u>RESPONSIBILITIES</u></b>
	<b>V. <u>SECURITY DESIGNATIONS</u></b>
	<b>VI. <u>PROCEDURES</u></b>
<b>Appendix</b>	<b><u>PERSONNEL SECURITY REPRESENTATIVES</u></b>

---

### **I. POLICY**

It is the policy of the Centers for Disease Control and Prevention (CDC)<sup>(1)</sup> that managers and employees protect classified material – including classified equipment or classified information, regardless of physical form, from inappropriate disclosure, loss, theft, espionage, sabotage, hacking, introduction into an unclassified computer system, or other mishandling. Managers must ensure that each employee who will need access to classified material has an established security rating and has received required clearances prior to providing that employee with access to any such material.

### **II. PURPOSE**

The purpose of this policy is to establish responsibilities, to describe various security designations, and to provide guidance for the logging, control, transmission, and accountability of classified material (Information protected under confidentiality and privacy laws are covered under other CDC policies).

### **III. DEFINITION OF CLASSIFIED MATERIAL**

The terms classified material, classified information, classified defense material, and other terms using the word "classified" refer to information requiring protection in the interest of national security, whether in paper or other physical form, or in electronic form.

### **IV. RESPONSIBILITIES**

Responsibility for the protection of classified material in the custody of CDC rests with each employee and manager having such information or knowledge no matter how it was obtained. Each individual will be directly responsible for adhering to all standards and procedures which are issued for protection of classified material. Anyone having knowledge of the loss, compromise, or possible compromise of any classified material should promptly report the circumstances to the appropriate security representative and /or the Internal Security Officer.

The following organizations have special responsibilities with regard to the protection of classified material.

**A. The National Security Agency (NSA)** has responsibility for Federal secure communications.

**B. The Office of the Chief Operating Officer (OCOO)** is responsible for CDC's physical security and secure communications facilities, and has oversight responsibility for handling, disseminating and storing classified material.

**C. The Office of Security and Emergency Preparedness (OSEP)** has primary responsibility for personnel security at CDC, ensuring forms are properly completed and processing requests for clearances. The Personnel Security/Drug Testing Section, OSEP maintain a current log for all CDC staff cleared to know, possess and / or handle classified material, and is the point of contact for verification of the level of clearance for CDC staff who may require such access.

## **V. SECURITY DESIGNATIONS**

### **A. Top Secret**

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include the disclosure of scientific or technological developments vital to national security, armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communications intelligence systems, and the revelation of sensitive intelligence operations.

### **B. Secret**

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, compromise of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security.

### **C. Confidential**

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength, focus, or objectives of United States military operations or forces, or performance characteristics, test data, design, and production data on munitions of war.

### **D. The word "Sensitive"**

This designation will be applied to material which is not entitled to protection or classification under Executive Order 12958, and its use signals the need to protect the material from inadvertent transmission outside of U.S. Government environments without additional protections, such as encryption. Within the CDC context, material bearing the "Sensitive" designation should be protected in the same manner as would identified health data.

## **E. Restricted Data**

This is an additional category of defense-related information, defined by the Department of Energy (DOE) as data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power. It is distinguishable from other classified material by the following marking which appears on the first page of the document (and the front cover, if there is one):

### **RESTRICTED DATA (RD) or FORMERLY RESTRICTED DATA (FRD)**

This document contains restricted data as defined in the Atomic Energy Act of 1954 as amended . Its transmittal or the disclosure of its contents in any manner to an unauthorized person is prohibited.

Restricted data may also carry the marking TOP SECRET, SECRET, or CONFIDENTIAL, as warranted by the security importance of the material.

## **VI. PROCEDURES**

### **A. Dissemination**

Employees and managers may not release classified material to another person without first determining whether that person is cleared to receive such material, has a "need to know" the information, and can properly store it. Security clearance information may be obtained from or through the CDC Personnel Security Representative. (See Appendix A for contact information.)

Classified material will be entrusted only to individuals whose official duties require knowledge or possession of such material. An employee or manager at CDC is not authorized to gain possession of classified material merely by virtue of his or her grade, rank, or position.

Public or private discussion of classified information with or in the presence or hearing of any person not authorized to have knowledge thereof is strictly forbidden.

Before any employee may have access to Restricted Data, they must have a special (Class "Q" or "L") clearance issued by the Department of Energy (DOE). Control and dissemination of Restricted Data will be made in accordance with the regulations of the DOE. The DOE "Q" clearance designation is the equivalent of a Top Secret clearance, and the DOE "L" clearance designation is the equivalent of a Secret clearance.

Employees and managers of CDC should not discuss or make available to foreign nationals or foreign governments any classified information.

It is permissible to make reference by unsecured telephones to nontelegraphic classified material if such references do not reveal the substance of the material under discussion. References to file numbers, dates, and subjects (provided the subject itself is not classified) may be made over an unclassified telephone if care is exercised not to reveal the substantive material.

Reference over telephone to the substance of classified and administratively controlled telegrams or documents may be made only when using a Secure Voice Unit. The CDC has the capability to talk at the **Top Secret** level<sup>(2)</sup> on the Secure Voice Units, as long as the key material for that device is at the Top Secret level. Individuals who desire to originate a call on the Secure Voice Unit must be verified by either the Logging Control Officer or Personnel Security Representative that they have appropriate security clearance.



## **B. Conferences and Meetings**

Conferences or meetings to discuss classified information should be scheduled in a protected setting. Every precaution will be observed to ensure that the participants are entitled to receive such information on a need-to-know basis, and that all participants possess suitable security clearances.

Before beginning the session in which classified materials will be discussed, the chair will confirm that all participants (those present, those connected via classified voice services, etc.) have appropriate clearances, meet other applicable restrictions (e.g., citizenship), have a need to know the specific information to be discussed, and have no electronic recording / transmitting devices, and that they are instructed on the procedures for control of any classified materials distributed during the session and of any notes taken by the participant relative to that session, regardless of when the notes are made.

Before a session is adjourned, the chair will assure that agreement is reached on the proper classification of the official minutes, if any, that classified materials are collected (if any were distributed) and that the participants are reminded of the proper safeguarding of any classified, highly sensitive or FOUO information remaining in his/her possession, including personal notations touching on such content.

## **C. Storage and Safekeeping**

Classified information, whether paper or electronic, will be held and stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in the HHS Security Manual will be observed at all times. Classified information, including Restricted Data, may not be converted to an electronic form, or be manipulated on a computer system, until written authorization to do so has been received from the original classifying authority or from the Internal Security Officer. Note that the CDC / ATSDR general computing system (LAN, workstations, server, mainframe, etc.) has NOT been authorized to create, receive, process, store, or transmit classified information.

Upon direct receipt of classified material, including material sent via secure fax, the individual will immediately deliver it to the Logging Control Officer or File Custodian for logging and preparation for processing.

Classified material should not be delivered to or left exposed in unoccupied offices. Under no circumstances should classified material be stored or placed in "plain view," in desk drawers, or in other readily accessible locations. Employees using classified material will take every precaution to prevent deliberate or casual inspection of it by unauthorized persons. All copies and informal material such as memorandums, notes, drafts, carbon copies, and carbon paper will be safeguarded by the rules prescribed for other classified material.

No classified material shall be allowed to remain outside the official security container (safe) overnight, nor will it be allowed to be taken home or carried onboard an aircraft or similar transportation. Material received, created, or checked out during the day must be returned to the Logging Control Officer or appropriate CIO custodians by 5 PM the same day.

When classified materials are in electronic form, the device / medium on which it is stored (floppy disk, hard drive, laptop / desktop computer, etc.) becomes a classified device at the same level as the highest classification of the information it contains. The device must be controlled, transported and stored in the same fashion as paper materials at that level. Before the device can be used in an environment of lesser classification, or released for use in an unclassified environment, all classified materials above the level of the destination environment must be

removed by an approved person, using an approved process, and the custodian of record must issue a written certification of its rating.

1. References to CDC include the Agency for Toxic Substances and Disease Registry (ATSDR)

2. Secure Voice Units will automatically seek the highest common classification level (up to the indicated desired level), e.g., if an individual with Top Secret security clearance and keys initiates a call at the Secret level and the other party has only Confidential security clearance and keys, then the connection will be limited to the Confidential level. Note also that a display on each unit will advise the parties as to the established level of clearance for the connection, and the identity of the other party to the conversation.

## **CLASSIFIED MATERIAL**

- Sections:**
- 1. PURPOSE AND SCOPE**
  - 2. POLICY**
  - 3. SECURITY DESIGNATIONS**
  - 4. RESPONSIBILITIES**
  - 5. ABBREVIATIONS AND ACRONYMS**
  - 6. REFERENCES**

### **1. PURPOSE AND SCOPE**

The purpose of this policy is to establish responsibilities, describe various security designations, and provide guidance for logging, controlling, transmitting, and maintaining accountability for classified material (information protected under confidentiality and privacy laws are covered under other CDC policies). This policy applies to all CDC and ATSDR personnel.

### **2. POLICY**

It is the policy of the Centers for Disease Control and Prevention (CDC)<sup>2</sup> that managers and employees protect classified material—including classified equipment or classified information—regardless of physical form, from inappropriate disclosure, loss, theft, espionage, sabotage, hacking, introduction into an unclassified computer system, or other mishandling. Managers must ensure that each employee who will need access to classified material has an active security clearance that has been processed and verified through the CDC Office of Security and Emergency Preparedness (OSEP)/Personnel Security Branch. Managers must also ensure employees have a “need to know” before access is provided to any classified material, and that the material is commensurate to the level of clearance of the individual.

### **3. SECURITY DESIGNATIONS**

#### **A. Top Secret**

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include the disclosure of scientific or technological developments vital to national security, armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communications intelligence systems, and the revelation of sensitive intelligence operations.

---

<sup>1</sup> Updated to reflect changes in policy format.

<sup>2</sup> References to CDC include the Agency for Toxic Substances and Disease Registry (ATSDR).



## **B. Secret**

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, compromise of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security.

## **C. Confidential**

This designation will be applied only to information or material when the unauthorized disclosure of such could reasonably be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength, focus, or objectives of United States military operations or forces, or performance characteristics, test data, design, and production data on munitions of war.

## **D. Sensitive But Unclassified Information (SBU)**

This designation will be applied to material which is not entitled to protection or classification under Executive Order 12958, and its use signals the need to protect the material from inadvertent transmission outside of U.S. government environments without additional protections, such as encryption. Information regarding the SBU designation is contained in a separate CDC policy.

## **E. Restricted Data**

This is an additional category of defense-related information, defined by the Department of Energy (DOE) as data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power. It is distinguishable from other classified material by the following marking which appears on the first page of the document (and the front cover, if there is one):

### **RESTRICTED DATA (RD) or FORMERLY RESTRICTED DATA (FRD)**

This document contains restricted data as defined in the Atomic Energy Act of 1954, as amended. Its transmittal or the disclosure of its contents in any manner to an unauthorized person is prohibited.

Restricted data may also carry the marking TOP SECRET, SECRET, or CONFIDENTIAL, as warranted by the security importance of the material.

## **F. Procedures**

### **(1) Dissemination**

Employees and managers may not release classified material to another person without first determining whether that person is cleared to receive such material, has a "need to

know” the information, the information is not classified higher than the individual’s clearance and can properly store it. Security clearance information may be obtained from or through a CDC OSEP personnel security representative (CDCPersonnelSecurity@cdc.gov).

Classified material will be entrusted only to individuals whose official duties require knowledge or possession of such material. An employee or manager at CDC is not authorized to gain possession of classified material merely by virtue of his or her grade, rank, or position. Public or private discussion of classified information with, or in the presence or hearing, of any person not authorized to have knowledge thereof is strictly forbidden.

Before any employee may have access to restricted data, they must have a special (Class “Q” or “L”) clearance issued by the Department of Energy (DOE). Control and dissemination of restricted data will be made in accordance with the regulations of DOE. The DOE “Q” clearance designation is the equivalent of a Top Secret clearance, and the DOE “L” clearance designation is the equivalent of a Secret clearance.

CDC employees and managers should not discuss or make available to foreign nationals or foreign governments any classified information. It is permissible to make reference by unsecured telephones to non-telegraphic classified material if such references do not reveal the substance of the material under discussion. References to file numbers, dates, and subjects (provided the subject itself is not classified) may be made over an unclassified telephone if care is exercised not to reveal the substantive material. Reference over telephone to the substance of classified and administratively controlled telegrams or documents may be made only when using a Secure Voice Unit. CDC has the capability to talk at the **Top Secret Secured Compartmented Information (SCI)** level on the Secure Voice Units<sup>3</sup>, as long as the key material for that device is at the Top Secret level. Individuals who desire to originate a call on the Secure Voice Unit must be verified by either the logging control officer or personnel security representative to ensure they have appropriate security clearance.

## **(2) Conferences and Meetings**

Conferences or meetings to discuss classified information should be scheduled in a protected setting. Every precaution will be observed to ensure that the participants are entitled to receive such information on a need-to-know basis, and that all participants possess suitable security clearances. Before beginning the session in which classified materials will be discussed, the chair will confirm that all participants (those present, those connected via classified voice services, etc.) have appropriate clearances, meet other applicable restrictions (e.g., citizenship), have a need to know the specific information to be discussed, and have no electronic recording / transmitting devices, and that they are instructed on the procedures for control of any classified materials distributed during the session and of any notes taken by the participant relative to that session, regardless of when the notes are made. Before a session is adjourned, the chair will assure that agreement is reached on the proper classification of the official

---

<sup>3</sup> Secure Voice Units will automatically seek the highest common classification level (up to the indicated desired level), e.g. if an individual with Top Secret security clearance and keys initiates a call at the Secret level and the other party has only Confidential security clearance and keys, then the connection will be limited to the Confidential level. Note also that a display on each unit will advise the parties as to the established level of clearance for the connection, and the identity of the other party to the conversation.

minutes, if any, that classified materials are collected (if any were distributed) and that the participants are reminded of the proper safeguarding of any classified, or SBU information remaining in his/her possession, including personal notations touching on such content.

### **(3) Storage and Safekeeping**

Classified information, whether paper or electronic, will be held and stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in the HHS Security Manual will be observed at all times. Classified information, including restricted data, may not be converted to an electronic form, or be manipulated on a computer system, until written authorization to do so has been received from the original classifying authority or from the internal security officer. Note that the CDC general computing system (LAN, workstations, server, mainframe, etc.) has NOT been authorized to create, receive, process, store, or transmit classified information.

Upon direct receipt of classified material, including material sent via secure fax, the individual will immediately deliver it to the logging control officer or file custodian for logging and preparation for processing. Classified material should not be delivered to, or left exposed in, unoccupied offices. Under no circumstances should classified material be stored or placed in "plain view," in desk drawers, or in other readily accessible locations. Employees using classified material will take every precaution to prevent deliberate or casual inspection of it by unauthorized persons. All copies and informal material such as memorandums, notes, drafts, carbon copies, and carbon paper will be safeguarded by the rules prescribed for other classified material. No classified material shall be allowed to remain outside the official security container (safe) overnight, nor will it be allowed to be taken home or carried onboard an aircraft or similar transportation. Material received, created, or checked out during the day must be returned to the logging control officer or appropriate coordinating center/office custodians by 5 PM the same day. When classified materials are in electronic form, the device/medium on which it is stored (floppy disk, hard drive, laptop / desktop computer, etc.) becomes a classified device at the same level as the highest classification of the information it contains. The device must be controlled, transported and stored in the same fashion as paper materials at that level. Before the device can be used in an environment of lesser classification, or released for use in an unclassified environment, all classified materials above the level of the destination environment must be removed by an approved person using an approved process, and the custodian of record must issue a written certification of its rating.

SCI material will only be stored in, and shall not leave, the Secured Compartmented Information Facility (SCIF).

## **4. RESPONSIBILITIES**

### **A. Employees and Managers with Access to Classified Information**

The responsibility for safeguarding classified material in the custody of CDC rests with each employee and manager having such information or knowledge, no matter how it was obtained.



Each individual will be directly responsible for adhering to all standards and procedures issued for protection of classified material.

## **B. All Employees**

Anyone having knowledge of the loss, compromise, or possible compromise of any classified material must promptly report the circumstances to the appropriate security representative and/or the internal security officer.

## **C. Office of Security and Emergency Preparedness (OSEP)**

**OSEP** is responsible for CDC's physical security and secure communications facilities, and has oversight responsibility for handling, disseminating and storing classified material. OSEP also has primary responsibility for personnel security at CDC, ensuring national security clearance background investigation forms are properly completed, and processed, and adjudicated. The Personnel Security/Suitability Branch, OSEP, maintains a current database for all CDC staff granted a security clearance and cleared to know, possess and/or handle classified material, and is the point of contact for verification of the level of clearance for CDC staff that may require such access.

## **5. ABBREVIATIONS AND ACRONYMS**

- A. CDC** – Centers for Disease Control and Prevention (including ATSDR)
- B. CUI** – Controlled Unclassified Information
- C. DOE** – U.S. Department of Energy
- D. LAN** – Local Area Network
- E. OSEP** – Office of Security and Emergency Preparedness
- F. SBU** – Sensitive But Unclassified Information
- G. SCI** – Secure Compartmented Information
- H. SCIF** – Secure Compartmented Information Facility

## **6. REFERENCES**

- A.** [Executive Order 12958, as amended](#)
- B.** [HHS National Security Information Manual](#)
- C.** [Access to Sensitive Compartmented Information and Communications Security Facilities at CDC](#)