Description of document:	Department of Health and Human Services (HHS) National Security Information Manual, February 1, 2005
Requested date:	07-June-2011
Released date:	13-June-2011
Posted date:	05-July-2011
Source of document:	Department of Health and Human Services FOIA Office Freedom of Information Officer Mary E. Switzer Building, Room 2206 330 C Street, SW Washington, DC, 20201 Fax: 202-690-8320 Online form: http://www.hhs.gov/foia/request/index.html

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C. 20201

Case No. 2011-0967 EW

June 13, 2011

This is in response to your June 7, 2011, Freedom of Information Act (FOIA) request for records pertaining to the National Security Information Manual.

The Office of the Security and Strategic Information located the 76 pages of record responsive to your request, which are enclosed in their entirety.

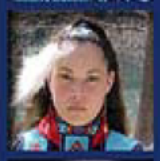
There are no fees for FOIA processing services in this instance, as billable costs do not exceed our $25 threshold for billing purposes.

Sincerely,

Robert Eckert
Director
FOI/Privacy Acts Division
Office of Public Affairs







Office of Security and Drug Testing

National Security Information Manual

February 1, 2005

FOR OFFICIAL USE ONLY
This information is intended for HHS use only. Disclosure is not expected to cause serious harm to HHS, and access is provided freely to all internal users via the organization's intranet.

U.S. Department of Health and Human Services

Table of Contents

Tables

U.S. Department of Health and Human Services

Subject: Safeguarding National Security Information - General Provisions

1-00-00 Purpose

The National Security Information Manual is the official Departmental document for providing policy and procedural guidance to the Department of Health and Human Services (HHS) employees and contractors who have access to classified national security information. This manual prescribes policy and responsibility for handling and safeguarding national security information in the possession of HHS. The guidance provided applies to those that are associated with or have a nexus to these programs.

1-00-05 Authority

Authority for the Manual derives from: Executive Order (EO) 12958, as amended; *Classified National Security Information Directive No. 1*; *Safeguarding National Security Information* (NSDD)-84, dated March 11, 1983; *Reporting Hostile Contacts and Security Awareness* NSDD-197, dated November 1, 1985; *Presidential Decision Directive* (PDD) 1; Security Awareness and Reporting of Foreign Contacts *PDD-12*, dated August 1993; National Industrial Security Program (NISP), Department of Defense (DoD) 5220.22-M with Change Two, dated February 2001; and the Agreement between DoD and HHS concerning the Industrial Security Program.

1-00-10 Policy

It is the policy of HHS to safeguard from unauthorized disclosure all national security information, also referred to as classified information, in the custody of the Department and its employees and contractors.

1-00-15 Applicability

The requirements of this Manual apply to all HHS employees and contractors whose duties require access to national security information.

Heads of Operating Divisions (OPDIVs) and Staff Divisions (STAFFDIVs) are authorized to issue supplemental guidance and instructions to facilitate implementation of the requirements of this Manual within their divisions. A copy of each supplement issued must be furnished to the Director, Office of Security and Drug Testing (OSDT), Immediate Office of the Secretary.

1-00-20 References

Classified National Security Information Directive No. 1 implements the provisions of EO 12958, as amended, and further sets forth guidance relating to original and derivative classification, downgrading, declassification, and safeguarding of national security information.

Safeguarding National Security Information NSDD-84 establishes procedures to safeguard against the unauthorized disclosure of national security information.

Reporting Hostile Contacts and Security Awareness NSDD-197 requires the creation and maintenance of a formalized security awareness program designed to protect classified, proprietary, and sensitive information from foreign sources, whether overt or covert. NSDD-197 also requires that procedures be established for employees to report any contacts with certain individuals and foreign nationals of certain specific countries.

Information Security Oversight Office (ISOO) Briefing Booklet, undated, provides information about the "*Classified Information Nondisclosure Agreement*," also known as the "SF 312."

ISOO Marking Guide, dated September 22, 2003, provides a general guide on the marking of classified national security information.

Security Awareness and Reporting of Foreign Contacts PDD-12 requires that government employees report all contacts with individuals of any nationality either within or outside the scope of the employee's official activities, in which illegal or unauthorized access is sought of classified or otherwise sensitive information, and when the employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.

HHS Instruction 731-1 provides policy and guidance on personnel security and security briefings of individuals requiring security clearances for access to national security information.

U.S. Security Authority for North Atlantic Treaty Organization (NATO) Affairs (USSAN) Instruction I-69, dated April 21, 1982, provides policy and guidance for the safeguarding of NATO classified materials.

National Telecommunications and Information Systems Security Policy (NTISSP) No. 3, dated December 19, 1988, was developed by the National Telecommunications and Information Systems Security Committee for the purpose of preventing the loss or unauthorized disclosure of U.S. classified cryptographic information.

Other classified directives and manuals of national security agencies provide policy and guidance for HHS personnel who are briefed into HHS special access programs.

1-00-25 Responsibilities

The Office of the Deputy Secretary

Under the authority delegated by the Secretary, the Deputy Secretary is the senior Department official responsible for the overall implementation of EO 12958, as amended; *Classified National Security Information Directive No. 1*, NSDD-84, NSDD-197, PDD-12; and similar future directives. Specific responsibilities include:

1. Issuing Department guidance to implement the provisions of EO 12958, as amended, the *Classified National Security Information Directive No. 1*, NSDD-84, NSDD-197, PDD-12, and future national security information directives.

2. Maintaining active oversight of the Department's Information Security Program for the safeguarding of national security information.

3. Making the final determination on a denial of a security clearance and/or access to classified information, based upon specific unfavorable information regarding the trustworthiness or loyalty of an HHS employee or contractor.

Heads of OPDIVs and STAFFDIVs

The Heads of OPDIVs and STAFFDIVs are responsible for ensuring that the requirements of this manual are implemented for their respective organizations. Specific responsibilities, which can be delegated, include:

1. Ensuring that all national security information received or handled within their organizations is properly safeguarded and controlled.

2. Ensuring that classified documents that are no longer required are properly destroyed in accordance with chapter 9-00 of this Manual.

3. Designating a senior management official to serve as the primary Classification Security Officer (CSO) for his/her respective organization to handle national security information responsibilities and one to serve as the Personnel Security Representative (PSR) to carry out the personnel security responsibilities. The same official may be designated to serve both functions.

4. Establishing a Logging Control Point (LCP) for any major office or organization which needs to store classified information and designating, in writing, a Logging Control Officer (LCO) or a separate Custodian of Classified Files, as needed.

5. Establishing additional written procedures, as necessary, to prevent unauthorized access to national security information and reduce the opportunity for the negligent or deliberate disclosure of the information.

Director of Office of Security and Drug Testing

The Director, OSDT is responsible for:

1. Overseeing the development of policy and procedures for the Department's classified information security program for safeguarding national security information.

2. Providing consultation and advice on the classified information security program to OPDIVs, STAFFDIVs, and other management officials.

3. Developing Department regulations to implement EO 12958, as amended, *Classified National Security Information Directive No. 1*, NSDD-84, NSDD-197, PDD-12, and other similar directives.

4. Developing and publishing security education material for use by CSOs, employees, and contractors who have been granted access to national security information.

5. Processing required personnel security investigations, in accordance with the HHS Personnel Security Handbook, and granting or denying security clearances to HHS employees and contractors.

6. Conducting national security information program reviews, assistance visits, inspections, and surveys within HHS to ensure compliance with this manual and authorities.

7. Receiving reports relating to the unauthorized disclosure and mishandling of national security information, and coordinating these, as necessary, with HHS and other Federal agency officials.

8. Providing security guidance and assistance to CSOs and PSRs and contractors as needed or requested.

9. Furnishing any required reports to the Director, ISOO.

10. Designating a Headquarters Top Secret Control Officer (TSCO) who shall be responsible for the control and accountability of all Top Secret documents in the custody of the Headquarters Top Secret Control Account. Prior to storage of Top Secret information in any OPDIV/STAFFDIV location, the secure room/facility must meet all requirements and be inspected and certified, in writing, by the Director, OSDT prior to use.

11. Approving requests for the establishment of a Top Secret Control Account and the assignment of a TSCO, whenever Top Secret information is routinely stored and received.

12. Designating an LCO and establishing an LCP to service the Immediate Office of the Secretary.

13. Appointing a Subregistry Control Officer and alternate(s) to be responsible for the Department's NATO Subregister.

14. Serving as an Original Classification Authority and the principal PSR for the Immediate Office of the Secretary.

Classification Security Officer

Designated OPDIV and STAFFDIV CSOs should meet a minimum training standard that includes Information Security Management, Classification Management and Special Access Orientation during a set period of time after their appointment. The CSO in each OPDIV and STAFFDIV has the following responsibilities:

1. Providing security advice on the handling of classified information to officials and employees of the organization.

2. Conducting an initial classification review of documents created by their organization and coordinate this review with OSDT. Conducting security inspections of all offices that store or handle classified information. The purpose of these inspections is to ensure that the office managers, supervisors, and employees responsible for classified material are in compliance with this manual.

3. Completing an audit of classified documents and reporting that data and other information on the HHS Annual Status Report on Classified National Security Information.

4. Advising OPDIV or STAFFDIV Heads on establishing an LCP and designating an LCO for their organization.

Personnel Security Representative

Each PSR has the following national security information responsibilities:

1. Ensuring that an employee or contractor has a legitimate need for a security clearance before signing the Request for Security Clearance, HHS Form 207, and forwarding it to OSDT.

2. Maintaining an up-to-date alphabetical list of all employees and contractors granted clearance for access to national security information. The list should include the level of clearance and the date of the last investigation on the cleared person.

3. Coordinating with the Director, OSDT, security matters affecting other Federal agencies (e.g., the Department of Homeland Security (DHS), the DoD, and the Department of Energy (DOE) access clearances).

4. Ensuring that initial, refresher, and termination security briefings are conducted, as required by the *HHS Personnel Security/Suitability Handbook,* and that required nondisclosure agreements and debriefing acknowledgments are signed and returned to the OSDT.

5. The PSR or a designated alternate will have the additional responsibility for review of all internal OPDIV or STAFFDIV pending contracts prior to the "Request for Proposal" (RFP) to determine whether or not the contract requirements meet the threshold of "classified contracts" as outlined in the NISP Operating Manual (NISPOM) or internal policies.

6. Conducting foreign travel security briefs for HHS employees and contractors with security clearances.

Supervisors

The primary responsibility of the supervisors is to ensure that national security information entrusted to their employees is safeguarded according to the policies and procedures contained in this manual. Supervisors whose employees routinely handle or store classified information are responsible for taking the following actions:

1. Assuring for the proper accountability, control, and storage of classified information, as outlined in chapters 6-00 and 7-00 of this Manual.

2. Designating, in writing, any employees authorized to receive and open outer and inner covers (envelopes) of security mail that is addressed to other cleared employees.

3. Assuring that no employee is permitted to have access to classified information until it has been officially determined that the employee has been granted the appropriate level of security clearance and has a

bonafide “need-to-know” for the information in the performance of his/her duties.

4. Assuring that the CSO, LCO, Custodian of Classified Files, and any of their employees who have been granted access to classified information are made aware of others in the organization (e.g., division) who have security clearances and meet the “need-to-know" requirement.

5. Reporting any violation of security procedures to their CSO promptly.

6. Establishing a system of security checks at the close of each working day to ensure proper safeguarding of classified information.

Logging Control Officer (LCO)

Each LCO has the following responsibilities:

1. Receiving all incoming accountable communications containing classified information.

2. Inspecting sealed envelopes or similar wrappings containing classified information for any evidence of tampering, damage, or unauthorized disclosure.

3. Matching the actual contents of an incoming package of classified material with the enclosed receipt.

4. Signing and returning to the sender enclosed receipts for classified material.

5. Maintaining an up-to-date *Classified Document Accountability Record*, HHS Form 208, and other documents showing disposition of classified materials.

6. Verifying through the PSR the security clearance level of recipients of classified information, including the clearance level of the Custodian of Classified Files storing the information.

7. Assuring prompt delivery of classified information to intended recipients who have the appropriate security clearance.

8. Handling the responsibilities of the Custodian of Classified Files unless there is a separately designated Custodian of Classified Files.

9. Taking prompt action on any downgrading and/or declassification notices received and coordinating with CSO on action taken.
10. Assuring that the appropriate secure method of transmission is selected and that the material is properly prepared for transmission.

11. Designating, either orally or in writing, an employee with a security clearance to act as a courier of classified documents and assuring the courier is properly briefed.

12. Destroying any unneeded classified documents in accordance with chapter 9-00 of this manual.

13. Providing training that includes safeguarding measures and classification document protection to any person that is designated as a custodian of classified files when such classified documents are stored in offices other than the Logging Control Point and that the custodian of classified files has at least a security clearance that is commensurate with the level of the classified documentation and no lower.

Custodians of Classified Files

When it is considered an absolute necessity that classified documents be stored in offices other than the LCP, separate Custodians of Classified Files shall be designated, in writing, to carry out the required duties. Employees appointed as Custodians of Classified Files are responsible for:

1. Providing protection for all classified information entrusted to their care.

2. Locking classified information in approved security containers whenever it is not in use or under the direct control of an authorized and cleared person.

3. Verifying the security clearance level of any person prior to giving that person access to classified information.

4. Returning to the LCP classified material designated for destruction.

5. Providing periodic inventory reports to the LCO.

Communication Security (COMSEC) Custodian

The COMSEC Custodian is responsible for the receipt, custody, issue, accountability, safeguarding and destruction of COMSEC material. The COMSEC Custodian is further responsible for the maintenance of up-to-date records and the submission of all required accounting reports. The COMSEC Custodian will be thoroughly familiar with the procedures for handling COMSEC material.

The COMSEC Custodian perform the following duties:

1. Protect COMSEC material charged to the COMSEC account and limit access to such material to individuals who have a valid need-to-know and, if the material is classified, are cleared to the level of the material.

2. Keep informed of any proposals or any new contracts to be serviced by the COMSEC account.

3. Receive, receipt for and ensure the safeguarding and accounting for COMSEC material issued to the COMSEC account.]

4. Maintain COMSEC accounting and related records.

5. Conduct an inventory semiannually/annually, and upon appointment of a new COMSEC Custodian, by physically sighting all COMSEC material charged to the account.

6. Perform routine destruction of COMSEC material when required, or effect other disposition of material as directed by National Security Agency (NSA) Central Office of Records (COR).

7. Submit transfer, inventory, destruction, and possession reports when required.

8. Beware at all times of the location of every item of accountable COMSEC material held by the account and the general purpose for which it is being used.

Employees

Any employee who obtains access to national security information is responsible for:

1. Protecting national security information, regardless of how it was received.

2. Reporting to their supervisor and/or their CSO the loss, or temporary loss, of control or possession of national security information.

3. Being familiar with and adhering to the provisions of this manual.

4. Ensuring that any classified information to which they may have access is never divulged, under any circumstances, to the media or other uncleared individuals (see Restrictions, Section 5-00-15).

1-00-30 Reporting Security Incidents

Any employee who has knowledge of the loss or possible compromise of classified information, or who discovers that a classified document is not being properly safeguarded, must immediately report the known circumstances to his/her immediate supervisor and CSO. The report should always be made in writing, unless for expediency purposes an oral report is authorized but should always be followed by a written report. This security incident must be immediately reported by the CSO to the Director, OSDT, who will report this to the agency that originated the information if there is reason to believe classified information has been lost or compromised.

The CSO must conduct a preliminary inquiry to determine the circumstances surrounding the reported security incident. The preliminary inquiry report must be in writing and sent to the Director, OSDT, within ten work days from the date of the incident. The inquiry report must not contain any classified information; however, it should include all relevant facts concerning the incident, including all steps taken to recover any missing classified documents.

After relevant facts are gathered the Director, OSDT, must promptly notify the agency that originated the classified information of any loss or possible compromise. If applicable, a damage assessment should be conducted and measures should be taken to negate or minimize any adverse effect of the loss or compromise.

Normal due-process procedures must be followed whenever an administrative action is contemplated against any HHS employee or contractor believed to be responsible for the compromise of classified information. Whenever a violation of criminal law appears to have occurred, the agency responsible for the damage assessment will coordinate with the Department of Justice to determine whether there will be criminal prosecution.

If there is no loss or possible compromise or unauthorized disclosure of classified information, the report of preliminary inquiry will be sufficient to resolve any procedural infraction, and when appropriate, support the taking of any administrative action. A procedural infraction is an incident which involves the misuse or improper handling of classified information where the action does not result in a possible compromise of classified information.

Additional procedures may be required when reporting a security incident involving special access program materials. The Director, OSDT, will provide those procedures and coordinate that inquiry.

1-00-35 Administrative and Criminal Sanctions

HHS employees may be subject to various administrative sanctions, including reprimand, termination of security clearance, or suspension or termination of employment, as appropriate, if they:

1. Refuse to cooperate in the conduct of a preliminary inquiry or formal investigation regarding a national security issue.

2. Knowingly, willfully, or negligently cause an unauthorized disclosure of classified information.

3. Display a lack of security responsibility relating to the proper handling and safeguarding of national security information.

4. Knowingly and only after having had the appropriate documented training, violate any provisions of EO 12958, as amended, and the references listed in 1-00-05 Authority section.

In addition to the administrative sanctions stated above, criminal sanctions may also be imposed. HHS employees may be subject to criminal sanctions as described under Sections 641, 793, 794, 798, and 952 of Title 18, United States Code (U.S.C.), Section 783 (b) of Title 50, U.S.C. or other appropriate statutes. Such sanctions may include penalties of up to a $10,000 fine, or imprisonment for ten years, or both (refer to 1800 *Briefing Booklet*).

1-00-40 Reporting Requirements

CSOs are responsible within their respective organizations for the submission of an annual National Security Information Data Report to the Director, OSDT. The format for the report will be furnished to the CSOs by the Director, OSDT, to request data needed for oversight responsibilities. Some of the data requested is used to report to ISOO and other agencies with national security responsibilities.

1-00-45 Suggestions

Suggestions about the HHS National Security Information Program, as set forth in this manual, should be directed in writing to the Director, OSDT. Suggestions for program improvement may be discussed with the Director, OSDT, at any time.

U.S. Department of Health and Human Services

Subject: Classification

2-00-00 Purpose

This chapter sets forth procedures for original classification, conveys duration of classification, and expresses guidelines for derivative classification and extending duration of classification.

2-00-05 Original Classification

In accordance to the authority provided by EO 12958, as amended, and other authority granting documents, as identified in Chapter 1, the Secretary of Health and Human Services (HHS) has been granted Original Classification Authority (OCA) at the Secret level of classification. The Secretary has delegated OCA to the Deputy Secretary and to the Director, Office of Security and Drug Testing (OSDT). Information may be originally classified as “Secret” only by those positions that have been granted original classification authority. Only the individual who occupies a designated position can exercise the authority inherent in the position.

Original classification is an initial determination that, in the interest of national security, information that has never been classified as “classified information” must be protected from unauthorized disclosure. In this initial determination, the original classifier is able to identify or describe why unauthorized disclosure of such information could cause damage to national security. Derivative classification authority permits an authorized individual to incorporate, paraphrase, extract, restate, or generate in a new form, information or material that has been identified as classified.

2-00-10 Classification Procedures

Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. The government must have some proprietary interest and ownership in the information; otherwise, classification is not an option.

Table 1. Categories Of Information For Classification

CATEGORIES OF INFORMATION THAT MAY BE CONSIDERED FOR CLASSIFICATION, AS SPECIFIED IN SECTION 1.5 OF EXECUTIVE ORDER 12958, AS AMENDED:	
(a) Military plans, weapon systems, or operations; (b) Foreign government information; (c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) Foreign relations or foreign activities of the United States, including confidential sources; (e) Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;	(f) United States Government programs for safeguarding nuclear materials or facilities; (g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) Weapons of mass destruction.

Under no circumstances should information be considered for classification to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security. Basic scientific research information not clearly related to national security should not be considered for classification.

Table 2. Factor To Be Consider For Classification

FACTORS THE OCA SHOULD CONSIDER:	
• Determining when and if information should be classified and for what duration; this requires balancing costs to protect against risk of information release;	• Selecting the appropriate level of classification to apply to information, based on a judgment as to the degree of damage that could be caused by unauthorized disclosure;

FACTORS THE OCA SHOULD CONSIDER:	
• Ensuring the advantages outweigh the disadvantages of classification; • Determining if the unauthorized disclosure of the information could result in damage to national security and being able to identify or describe such damage;	• Determining the appropriate declassification instructions to apply to information; and • Communicating the classification decision to the individuals, who will likely be in possession of that information or by making sure that the document is properly marked.

EO 12958, as amended, outlines a uniform system for classifying, safeguarding, and declassifying national security information. Designed to prevent overclassification of Federal documents through improved standards for government classifiers, it promotes openness by emphasizing declassification of documents, especially for specific records of permanent historical value.

2-00-15 Duration of Classification

When originally classifying information, the OCA must determine the duration of the security classification period. The OCA should attempt to identify a future date or event for declassification that will occur in 10 years or less. This declassification date or event will be assigned to the information to mark the end of the security classification period. If unable to determine a date or event of less than 10 years, the OCA should assign a declassification date that is 10 years from the date of the original classification decision. For most original classification actions, 10 years is the norm. Should the OCA determine that the nature and sensitivity of the information must be protected for a period greater than 10 years, then the information should be marked for declassification after 25 years from the original date of classification, but not longer than its destruction date. If the information to be classified is deemed to have permanent historical value, the period of classification cannot exceed 25 years from the date of origination.

Information will be classified as long as it is required by national security consideration; such determinations will only be made by the OCA. Information cannot be classified beyond the time needed to protect national security. Overtime,

there is a possibility that the information's sensitivity could decrease and the level of classification could be lowered.

2-00-20 Communicating the Classification Decision

An OCA, who has made a decision to classify original information, is responsible for communicating that decision to persons who will likely be in possession of that information. This will be accomplished by issuing classification guidance or by making sure that a document containing the information is properly marked to reflect the decision. Marking requirements for classified material, including page and paragraph markings, are covered in Chapter 4 of this manual.

2-00-25 Classification Challenges

Authorized holders of information classified by HHS who, in good faith, have substantial reason to believe that the information is improperly or unnecessarily classified, should communicate that belief through their CSO and to the Director, OSDT, who will submit it to the OCA for review and bring about any necessary correction. This can be completed informally or by submission of a formal challenge to the classification as provided for in EO 12958, as amended, and this Manual. Informal questioning of classification is encouraged before resorting to formal challenge. An authorized holder is any person who has been granted access to specific classified information being challenged. The Director, OSDT is the point of contact to communicate informal classification challenges and formal classification challenges. The Office of the Deputy Secretary will establish an impartial review panel, should the authorized holder choose to communicate a formal challenge.

No individual will be subject to retribution for bringing such a formal challenge. EO 12958, as amended, established the Interagency Security Classification Appeals Panel (ISCAP). Each individual, whose formal challenge is denied, will be advised that he/she may appeal to ISCAP. One of the roles of ISCAP is to decide appeals by authorized holders of the information who have made a formal classification challenge, as described in this section.

Likewise, the public has the ability to challenge the classification level of classified US Government documents by requesting that a specific document be reviewed for declassification and release to the public.

2-00-30 Derivative Classification

Derivative classification is the process of determining whether information that is to be included in a document or material has been classified and, if it has, ensuring that it is identified as classified information by marking or similar means. Employees need not possess original classification authority to reproduce, extract, paraphrase, restate, summarize, or to apply classification markings derived from

source material or as directed by a classification guide for documents based on other agency's classification. For HHS produced documents, derivative classification authority must have been granted. Producing photo simile or otherwise mechanically reproducing classified material is not derivative classification.

The Secretary has only delegated derivative classification authority for HHS developed information, using HHS security classification guides, to the heads of the National Institutes of Health (NIH), Centers for Disease Control and Prevention (CDC), and the Food and Drug Administration (FDA). CSO's and their alternates are delegated derivative classification authority using classified source documents.

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information that is already classified by an OCA, or in accordance with an authorized classification guide.

The overall classification markings and portion (i.e., paragraph) markings of the source document should supply adequate classification guidance to the person marking the extraction. If portion markings or classification guidance is not found in the source document, and no reference is made to an applicable classification guide, guidance must be obtained from the originator of the source document.

2-00-35 Classification Guide

A classification guide is written guidance that is issued by an official, exercising OCA over particular programs, projects, or classes of documents. OPDIVs will use a classification guide to facilitate the proper and uniform derivative classification of information. The guide will conform to standards contained in directives and regulations issued under EO 12958, as amended, and this regulation.
The primary purpose of a classification guide is to ensure that proper and uniform classification markings are applied to derivatively-classified information.

An OPDIV can develop a classification guide and submit it to the Director, OSDT for review and forward to HHS OCA for approval. Periodically, the Director, OSDT will review the classification guide for updates.

U.S. Department of Health and Human Services

Subject: Declassification and Downgrading

3-00-00 Purpose

The purpose of this chapter is to provide guidance relating to the declassification and downgrading of information that was originated by HHS, other agencies, and predecessor HHS agencies.

3-00-05 Declassification and Downgrading Authority

The following officials are authorized to declassify and downgrade information:

A. The Secretary with respect to all information over which HHS exercises final classification authority;
B. The original classification authority, as designated by the Secretary, a successor to the original classification authority, or a supervisor of either;
C. The official of the originating agency who authorized the original classification for classified information originated by other agencies; or
D. The Director, OSDT, with respect to all classified documents originated by a HHS-predecessor agency and being retained for some official reason, following the coordination with the OPDIV or STAFFDIV that has subject matter interest in the documents.

If it is determined that some information meets the current criteria of Section 2-00-15, or there is some doubt concerning its classification, the information must be promptly transmitted in the manner required by Chapter 8-00, to the Director, OSDT, for review and transmittal to an agency that has appropriate subject matter interest and original classification authority. That agency will decide whether to declassify, upgrade, downgrade, or extend the initial classification level of the document.

Authority to downgrade or declassify must not be mistaken with the authority of the CSO. The CSO may downgrade or declassify information as directed by a

classification guide, continued protection guidelines, or declassification instructions on a document.

3-00-10 Annual Review Guidelines

The CSO of each organization will conduct an annual review of all classified documents in their possession and control to identify documents that require declassification, downgrading, or destruction. This review is to be accomplished prior to completion of the HHS Annual Status Report on Classified National Security Information. In accordance with Section 3.4 of EO 12958, as amended, the following will be followed:

Table 3. Annual Review Guidelines For Classified Documents

ANNUAL REVIEW GUIDELINES FOR CLASSIFIED DOCUMENTS
A. All classified information, in which the information's sensitivity has ceased, should be destroyed and disposed of in the manner prescribed by Chapter 9-00;
B. Documents classified by other agencies under predecessor EOs that are marked for automatic downgrading or automatic declassification on a specific date or event should be downgraded and declassified according to the instructions on the face of the documents; and
C. Documents classified by other agencies under predecessor EOs that are not marked for automatic downgrading or declassification on a specific date or event must not be downgraded or declassified without authorization, in writing, from the original classification authority. HHS will alert the originating agency and seek instruction regarding the handling and disposition of pertinent records.

3-00-15 Automatic Declassification

All HHS classified documents that have been classified for more than 25 years and have been determined to have permanent historical value will automatically be declassified on December 31, 2006, regardless of whether a document review has been conducted. All classified documents will have a maximum classification life of 25 years from the date of its original classification, unless guidance from the Secretary has determined that the document may be exempt from automatic declassification.

3-00-20 Mandatory Review Requests For Declassification

In accordance with Section 3.5 and 3.6 of EO 12958, as amended, a United States citizen or immigrant alien, a Federal agency, or a state or local government may request a review for declassification of information that was originally classified by HHS or its predecessor agencies under prior EOs. The request to release information does not need to identify the date or title of the information; however, it should be particularly specific to the information to enable HHS personnel to locate the sought after information with a reasonable amount of effort. Requests should be submitted to the Director, OSDT either as a mandatory review request or under the Freedom of Information Act (FOIA) review process. If the request is submitted as both processes, then the Director, OSDT will require the requestor to select only one process. If the requestor does not make a selection, the default process chosen will be FOIA, unless the information requested is subject only to a mandatory review.

The Director, OSDT, will coordinate the review request for declassification with the office in charge of FOIA/Privacy Act (PA) requests, the Office of the Assistant Secretary for Public Affairs, in an attempt to locate the requested classified information. Responses to requests will be governed by the amount of search and review time required to process the request. However, in the interest of being responsive to such requests, the IOS, STAFFDIV, or OPDIV office that has primary interest in the subject matter must be contacted in an attempt to locate and review the requested information. Results of the review, including recommendations and a copy of the requested information, or a request for additional time, must be furnished to the Director, OSDT, who is to notify the requester accordingly or inform the requester of the additional time needed to process the request. EO 12958, as amended, requires that agencies make a final declassification determination within one year from the date of receipt, except in unusual circumstances.

The IOS, STAFFDIV, or OPDIV office should make a prompt recommendation to the Director, OSDT, for the requested information or portions of information to be declassified. When the requested information cannot be declassified in its entirety, reasonable efforts should be made to release those declassified portions that constitute a coherent segment. If the information may not be released in whole or in part, the action office must provide the reasons for denial. When the classification of the requested information is a derivative decision, based on classified source material of another agency, the information must be provided to that agency for review and comment.

Upon receipt of the declassification review recommendation, the Director, OSDT, must make the declassification determination after contacting the originating

agency, when necessary, and furnish any declassified information to the office handling FOIA/PA requests for a determination regarding release of the information.

When HHS receives a mandatory declassification review request for classified records that were originated by another agency and in the custody of HHS, the request is to be submitted to the Director, OSDT, who will refer the request and the pertinent records to the originating agency. Nevertheless, if the originating agency had previously agreed that HHS, as the custodial agency, may review its records, the Director, OSDT, will review the requested records in accordance with declassification guides or guidelines provided by the originating agency. The Director, OSDT, will communicate to the requestor, the originating agency's declassification determination.

The Director, OSDT, must declassify all HHS-originating information by marking it to reflect the change, as well as the authority for and date of the declassification method. If the review request for declassification is denied, in whole or in part, the Director, OSDT, must notify the requestor of the information in writing of the final determination and the reasons for any denial, as well as the right to appeal the determination within 60 working days of receipt of the denial.

In accordance with Section 3.5 and 3.6 of EO 12958, as amended, HHS may require a fee for declassification review requests. A requestor may appeal to the Deputy Secretary when the requested information is not declassified and released in whole. Below are the Deputy Secretary's appeal review procedures:

Table 4. Deputy Secretary's Appeal Review Procedures

DEPUTY SECRETARY'S APPEAL REVIEW PROCEDURES
A. The Deputy Secretary will normally make a determination within 30 business days following the receipt of an appeal. If additional time is required to make a determination, the Deputy Secretary will notify the requestor of the additional time needed and provide the requestor with the reason for the extension. If continued classification of the information is required, the Deputy Secretary will notify the requestor in writing of the final determination and the reason for any denial.
B. During the appeal review, the Deputy Secretary may overrule any previous determination in whole or in part when, in his/her judgment, continued protection of information is no longer required in the interest of the national security. If the Deputy Secretary determines that the information no longer requires classification it will be declassified and, unless it is otherwise exempt from disclosure under the FOIA/PA, released to the requestor. The Deputy Secretary will advise the original HHS reviewing office of his/her decision.

Each individual whose review request for declassification is denied will be advised that he/she may administratively appeal a final agency decision to ISCAP. EO 12958, as amended, established ISCAP as a venue by which individuals whose review request for declassification is denied, could appeal the final agency decision.

3-00-25 Declassification Guide

A declassification guide is written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified. In accordance with Section 3.3 of EO 12958, as amended, this guidance is issued by an official exercising OCA over particular programs, projects, or classes of documents. OPDIVs and STAFFDIVs will use a declassification guide to facilitate the proper and uniform declassification of information. The guide will conform to standards contained in directives and regulations issued under EO 12958, as amended, and this regulation.

An OPDIV or STAFFDIV can develop a declassification guide and submit it to the Director, OSDT, for review and forward to HHS OCA for approval. Periodically, the Director, OSDT, will review the classification guide for updates. In place of a separate declassification guide, declassification guidance can be included in a classification guide for a similar, current system, plan, program, or project.

U.S. Department of Health and Human Services

Subject: Marking Original and Derivatively Classified Documents

4-00-00 Purpose

This chapter provides specific guidance for marking documents containing original or derivatively classified information in accordance with the *Classified National Security Information Directive No. 1*.

4-00-05 Original Classification Identification and Markings

Classified information must be marked at the time of original or derivative classification to inform and warn the holder of the information about its sensitivity. An official who exercises original classification authority under EO 12958, as amended, is responsible for ensuring that the proper classification markings are applied. Markings must be applied uniformly and conspicuously to ensure there is no doubt as to the classification level, the reason for classification, the duration of classification, and the authority or derivative source for classification. Following the marking guidance from the *ISOO Marking Guide*, the following primary markings must be applied to the face of each originally classified document (i.e., disks, documents, etc.):

Table 5. Primary Markings of Original Classification

Primary Markings of Original Classification
• Classification Authority — The name or personal identifier and position title of the OCA on the "Classified By" line. • Agency and Office of Origin — The office originating the document must be identified and follow the name on the "Classified By" line. • Reason for Classification — The reason(s) for the decision to classify the material must be stated. The OCA must at least provide a brief reference to the pertinent classification category(ies) of the EO, as described in Section 2-00-10.

Primary Markings of Original Classification
• Declassification Instructions — The duration of the original classification decision must be stated on the "Declassify By" line. The appropriate declassification instructions also need to be identified (i.e., a specific date or event within 10 years, a date that is 10 years from the original decision, or a date not to exceed 25 years from the date of original classification).

Following the guidance in the *ISOO Marking Guide* the document to be originally classified will ensure the following areas are addressed: overall marking, portion marking, classification extensions, and marking information exempted from automatic declassification at 25 years.

4-00-10 Derivative Classification Identification and Markings

In accordance to Section 2.1 of EO 12958, as amended, derivative classified documents will follow the marking instructions for originally classified documents, as described in Section 4-00-05. However, the information for the markings will be carried forward from the source document or taken from instructions in the appropriate classification guide and *ISOO Marking Guide*. Original or derivative classifiers are accountable for the accuracy of their classification decisions. Proper marking of classified information serves to alert holders of special access, control or safeguard requirements, and make information useful to recipients.

Table 6. Primary Markings of Derivative Classification

Primary Markings of Derivative Classification
• Source of Derivative Classification — Identify the source data on the "Derived From" line, including the agency, the office of origin, and the date of the source or guide. Should the document be derived from multiple sources, then the "Derived From" line will state "Derived From: Multiple Sources." Retain a list or copies of all the source documents used in derivatively classifying the document. • "Derived From: Multiple Sources" Document— When a document that is marked as being from "Derived From: Multiple Sources," cite the source document on the "Derived From" line instead of using the phrase "Multiple Sources." • Reason for Classification — The reason is not required to be transferred from the original classification decision. • Declassification and Downgrading Instructions — Carry over the "Declassify On" line from the source document. When multiple documents are used as sources, use the longest duration date of its sources. Documents that are not to be declassified automatically have instructions indicating the dates or events for automatic

Primary Markings of Derivative Classification
declassification or downgrading, or the notation Originating Agency's Determination Required (OADR). • Overall Marking — Mark the derivatively classified document with the highest level of security classification ("Top Secret," "Secret," or "Confidential") included in the source document. • Portion Marking — Mark each portion of the derivatively classified document in accordance to the *ISOO Marking Guide*.

4-00-15 Marking Prohibitions

In accordance to Section 1.6 of EO 12958, as amended, and the *ISOO Marking Guide*, the highest level of security classification ("Top Secret," "Secret," or "Confidential"), extracted from a source document or determined from an originating agency's classification guide, must be marked or stamped at the top and bottom on the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover or page.

Markings other than "Top Secret," "Secret," or "Confidential", such as "For Official Use Only," "Sensitive But Unclassified," "Limited Official Use," or "Sensitive Security Information" are not to be used to identify classified national security information. Each interior page must be marked at the top and bottom according to the highest classification of the extracted information (e.g., "Top Secret," "Secret," "Confidential," or "Unclassified"). Each section, part, paragraph, subparagraph, or

similar portion of a derivatively classified document must be marked to show the level of classification assigned to the specific information.

4-00-20 Transmittal Documents

A transmittal document is to be marked in the manner prescribed by Section 4-00-5 and 4-00-10 above, to show the highest level of classification of the information contained in the transmittal itself, if applicable, and in the material attached, as well as contain a legend showing the classification of the transmittal document standing alone. A transmittal document that does not contain classified information should be marked with the highest level of classification of the attachments. The marking should appear at the top and bottom of all pages. In addition to the classification marking, type the statement, "Unclassified When Classified Enclosure Removed" or

"Upon Removal of Attachments, This Document is (Classification Level)" at the bottom margin of the first page.

4-00-25 Foreign Government Information

In compliance with Section 1.6 of EO 12958, as amended, U.S. documents that contain foreign government information are to be marked on the front, "This Document Contains (indicate country of origin) Information." The portions of the document that contains foreign classified information are to be marked to identify the classification level and the country of origin, using accepted country code standards. No US document is to be downgraded below the highest level of foreign government information contained in the document, nor is it to be declassified without the written approval of the foreign government that originated the information.

In the event that the foreign government information must be concealed, the markings described in this section are to be disregarded and the document is to be marked as if it were wholly of the US origin.

4-00-30 Working Papers

Working papers include classified notes, drafts, or similar items that are not finished classified documents, regardless of the media (i.e., disks, documents, etc.). Working papers containing classified information must be marked with the overall highest classification of any information contained in them, dated when created, and destroyed when no longer needed, regardless of status. For disks and other removable media, use SF 706 (Top Secret), SF 707 (Secret), or SF 708 (Confidential) labels on disks and removable drives. Ensure that all documents on the disk or drive are properly marked.

Working papers or the creation of working papers intended to be "classified documents" will not be produced outside of the OPDIV or STAFFDIV secure area such as a Sensitive Compartmented Information Facility (SCIF) without the knowledge or consent of the OPDIV/STAFFDIV CSO. When working papers are to be released by the originator outside the originating activity, retained for more than 180 days from the date of origin, or converted into a permanently held document, normal marking rules apply. Finished documents are classified documents that contain all required markings and may be approved for official release outside HHS (e.g., transmission).

Oversized and bulky material (e.g., equipment and facilities) are to be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification.

U.S. Department of Health and Human Services

Subject: Access and Dissemination

5-00-00 Purpose

This chapter provides general guidance for granting access to classified information.

5-00-05 Security Clearance and Access

No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with EO 12958, as amended, and possesses a need-to-know. The provisions for obtaining and granting a security clearance for Federal Government employees is different than that of those who may be employed as contractors to the Federal Government. All Federal Government employees requesting access to classified information based on a need- to-know will have a security clearance that is at least commensurate with the level of access information requested. This process implies that the employee is required to, at a minimum; undergo the request for security clearance process through the individual OPDIV or STAFFDIV. All non-Federal employees who are identified outside the Federal Government employment scope as contractor's will abide by the agreement between DoD and HHS concerning NISP. PSR's will ensure that the agreement as written is enforced and that mechanism for tracking and documenting requests for access is in place and shared with CSO's.

The need for access means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

The Director, OSDT, adjudicates the completed background investigation and determines whether to grant the requested security clearance. The Director, OSDT, grants the clearance by signing the HHS 207 form and forwarding a copy to the PSR who requested the clearance action. The PSR assures that the individual is briefed

about security requirements and signs the *Classified Information Nondisclosure Agreement Standard Form* (SF 312). The signed original HHS 207 form and SF 312 are maintained in the official security file at OSDT. The number of employees cleared and granted access to classified information must be maintained at the minimum number that is consistent with operational requirements and needs.

Every person who has met the standards for access to classified information in accordance to Section 4.1 (a) of EO 12958, as amended, and to Section 5-00-05 of this manual, will receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

No one has a right to have access to classified information solely by virtue of title, position, or level of security clearance. The final responsibility for determining whether the individual has been granted the level of security clearance needed, and whether an individual requires access to classified information, rests with the individual who has possession, knowledge, or control of the classified information, and not upon the prospective recipient. Verification of a security clearance may be made through the individual's PSR provided the PSR has received a delegation of authority by HHS to transmit the clearance through whatever appropriate means are necessary. A request may also be made through the Director, OSDT if required.

In addition to a security clearance, a person must have a need-to-know the classified information in connection with the performance of official duties. The need-to-know is established by the individual who has possession, knowledge, or control of the classified information based on the official duties of the position that the employee occupies. Persons who disclose classified information must advise recipients of the classification level of the information.

5-00-10 Downgrade or Withdrawal of Access

A security clearance may be downgraded or terminated for administrative reasons unrelated to an adverse security determination or when in the execution of an individual’s position a clearance is no longer needed. Just as the immediate supervisor or program manager is responsible for requesting a security clearance, he or she is also responsible for advising the Director, OSDT, through their PSR whenever an administrative downgrade or termination of security clearance is appropriate based on a changed need-to-know. After notification to the individual, the Director, OSDT, may administratively withdraw or downgrade the clearance. If the clearance is withdrawn, the individual should be debriefed and asked to sign the Security Debriefing Acknowledgment on the lower portion of the back of the

Classified Information Nondisclosure Agreement (SF 312). The SF 312 with original signature must be sent to the Director, OSDT, for maintenance.

The Director, OSDT, may withdraw clearance when it is determined that there is a question regarding the individual's trustworthiness. Also, the Director, OSDT, may administratively withdraw a clearance whenever a previously cleared individual refuses to comply with reinvestigation requirements. The clearance, subsequently, may be reissued based on compliance with reinvestigation requirements and a redetermination of the individual's trustworthiness and identifiable need for access. The provisions and processes of EO 12968, as amended, Access to Classified Information, are to be followed when a downgrading or administrative termination of a security clearance is either needed or required. Security Clearance Denials or Revocations will follow the review proceedings of eligibility for access as outlined in EO 12968, as amended, Section 5.2.

A security clearance may be revoked by the Deputy Secretary when it is determined that such clearance or access is no longer consistent with the interests of national security due to a question regarding the individual's trustworthiness or loyalty. Due process procedures must be followed when processing a revocation of a security clearance for cause.

Individuals who are being denied a security clearance or having their clearance revoked because they do not meet access eligibility standards, must be given specific appeal rights, as stipulated in EO 12968, Section 5.2, *Review Proceedings for Denials or Revocation of Eligibility for Access*. The Director, OSDT, will coordinate the appeal process.

Whenever a security clearance is withdrawn or revoked the employee should receive the termination briefing prescribed by the *HHS Personnel Manual*. The Director, OSDT, will notify the employee's PSR about the termination of the security clearance so that the PSR can inform the employee's supervisor, CSO, and others who have a need to know. When misconduct is reported to the servicing human resources office, and the individual occupies a sensitive position, the servicing human resources specialist should contact the servicing security officer immediately.

5-00-15 Restrictions

Classified information must be discussed only with persons who are properly identified, have the proper security clearance, and have a valid need-to-know the information in performance of official duties. Discussion of classified information in

homes with relatives or friends, in public places, on public conveyances, or any place where unauthorized persons may have access, is strictly prohibited. Classified information must not be released to employees or other persons for their private use. Classified information must not be removed from official premises without proper authorization.

Employees must not comment on published news articles concerning information that they know or think to be classified. Publication by a news media does not constitute proper authority for declassification, as it is often the product of astute guessing.

Standard telephones, inter-office communication systems, and unsecured mobile wireless telephones must not be used for purposes of discussing classified information. A number of secure telephones are available throughout HHS for use by cleared employees; the Director, OSDT, can provide their location.

5-00-20 Dissemination of Other Agency Information

Classified information originated in another agency must not be disseminated outside HHS without the consent of the originating agency. Such consent must be maintained in writing as a matter of record. This restriction does not apply to the authorized dissemination within the HHS, unless such a limitation is stated on a specific classified document.

5-00-25 Dissemination of HHS Information

Classified information originated by HHS, under the authority of current or prior EOs, must not be disseminated outside of the Department until the information has been reviewed for downgrading or declassification in accordance with Chapter 3-00. An official or employee leaving HHS may not remove classified information from the Department's control.

5-00-30 Access by Foreign Nationals, Foreign Governments, and International Organizations

No HHS official or employee is authorized to discuss or make available any classified information to foreign nationals, foreign governments, or international organizations, except for the allowances provided by Section 2.6.7 of EO 12968, as amended. Refer requests for such information to the originating agency and to the Director, OSDT, for information originally classified by the Department.

U.S. Department of Health and Human Services

Subject: Custody, Accountability, and Reproduction

6-00-00 Purpose

The purpose of this chapter is to provide instructions relating to the custody, accountability, and reproduction of classified information in accordance with the *Classified National Security Information Directive No. 1*, *Subpart D*.

6-00-05 Custody of Classified Information

Any person who has possession of, or is charged with the responsibility of custody of classified information, is responsible for protecting and accounting for that information. The following measures are to be taken to protect classified information:

Table 7. Measures To Protect Classified Information

MEASURES TO PROTECT CLASSIFIED INFORMATION
1. While in use, classified documents (i.e., disks, documents, etc.) must be kept under constant observation by a cleared person or properly stored in accordance with the guidance in Chapter 7-00.
2. An employee who receives a classified document (in any form) and has no authorized storage container available must either return the classified information to the sender, arrange with another office to store the document in a manner that will meet the storage requirements as outlined in Chapter 7-00, or destroy it by an approved method in accordance with Chapter 9-00. Under no circumstances should classified information be left unattended, be left in an unauthorized storage container, or be left in the custody of a person who does not have the proper security clearance and an established need-to-know.
3. Classified information must only be delivered to or left with cleared recipients.
4. Occupants of an office must ensure that uncleared persons assigned to or visiting the office do not take or read classified information, overhear classified discussion, or have

MEASURES TO PROTECT CLASSIFIED INFORMATION
visual access of classified information. 5. Classified information must be discussed only with cleared persons who have the need-to-know, and must not be discussed in public or other places where it may be heard by unauthorized persons. 6. Classified information must not be checked with baggage or left in such places as private residences, locked or unlocked automobiles, hotel rooms, hotel safes, aircraft, train compartments, buses, public lockers, etc. 7. Classified information must not be read, studied, displayed, used, or discussed in any manner in a public conveyance or place.

6-00-10 Accountability of Classified Information

Office managers and supervisors, whose employees handle or store classified information, must ensure that procedures are established for the accountability of Top Secret and Secret information. Such procedures should provide for tracing the movement of classified information, limiting dissemination, retrieving documents promptly, detecting the loss of information, and preventing excessive production and reproduction of documents. At a minimum, the following accountability procedures should be established for each level of classification:

Table 8. Accountability Procedures

ACCOUNTABILITY PROCEDURES
Top Secret Information 1. A designated CSO is to administer each authorized Top Secret Control Account by using a *Classified Document Accountability Record*, HHS Form 208, to track each Top Secret document. Only Top Secret documents should be accounted for on a single HHS Form 208. 2. A *Classified Document Receipt*, HHS Form 25, must-be used each time Top Secret documents are transmitted from one individual, office, organization, or agency to another. HHS Forms 208 and 25 should be destroyed in five years after the Top Secret documents are destroyed, transferred, or downgraded. **Secret and Confidential Information**

ACCOUNTABILITY PROCEDURES

1. A separate HHS Form 208 must be used to account for all Secret documents received by an HHS office. HHS Form 25 must be used as a receipt for Secret documents whenever they are transmitted from one individual, office, organization, or agency to another. These HHS Forms 208 and 25 should be destroyed two years after the related documents are destroyed, transferred, or downgraded.

2. Accountability records and document receipts are not required for Confidential information, although their use is a good security practice to aid in controlling these classified documents. However, Confidential information must be handled, stored, and transmitted in accordance with the provisions of this manual. Confidential documents can be accounted for on the same HHS Form 208 used for Secret. The *Classified National Security Information Directive No. 1,* further sets forth guidance relating to original and derivative classification, downgrading, declassification, and safeguarding of national security information.

3. The same HHS Form 25 can be used when Confidential documents are being sent with Secret ones.

Working Papers

1. Working papers are documents (i.e., disks, documents, etc.), including drafts, that are created to assist in the formulation and preparation of a finished document. Working papers containing classified information must be handled and safeguarded like normal classified information.

To prevent the inadvertent or unauthorized disclosure of Top Secret, Secret, and Confidential classified information, it must be protected by a cover sheet. *Top Secret Cover Sheet* (SF 703), *Secret Cover Sheet* (SF 704), or *Confidential Cover Sheet* (SF 705) must be used for this purpose (see Exhibits). An SF 703, 704, or 705 cover sheet must be affixed to the front of the classified document and remain attached until the document is destroyed. At the time of destruction, the forms should be removed and, depending upon their condition, reused.

If an office routinely receives numerous Confidential cable messages (e.g., those from the State Department) they can be kept in separate file folders with a SF 705 attached to the front of each folder.

6-00-15 Production and Reproduction of Classified Information

Production and reproduction of classified information is to be held to the minimum number of copies needed consistent with operational requirements. In addition, production and reproduction of classified information is to be accomplished by authorized personnel.

Only OSDT-approved automated information systems may be used to produce classified information. Automated systems or stand-alone computers used to process classified information must have been cleared and designated for use for classified information, in writing, from the Director, OSDT, or designated CSO.

Consistent with Section 4.1 of EO 12958, as amended, uniform procedures must be established to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that prevent access by unauthorized persons and ensures the integrity of the information.

The computer hard drives or disks used in typing classified information must be treated as classified material, marked with the appropriate markings, and safeguarded after use or properly destroyed. A standalone printer must be dedicated for the production of classified materials and should be properly marked.

Copies of classified information are to be subject to the same controls as the original information. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged. All classified documents should be subject to the following reproduction restrictions:

Table 9. Reproduction Restrictions

REPRODUCTION RESTRICTIONS
1. The designated, cleared personnel should be authorized to reproduce classified documents.
2. The number of copies should be kept to a minimum to decrease the risk of compromise and reduce storage costs. Any stated prohibition against reproduction must be strictly observed.
3. Reproduction equipment used to reproduce classified documents must be specifically designated and the following rules should apply:

REPRODUCTION RESTRICTIONS

a. Make sure that the number of copies programmed are actually delivered.

b. Reproduce only the number authorized.

c. Account for all copies, including originals before leaving the machine.

d. Ensure that all classifications and any special markings appear on reproduced copies.

e. If the machine malfunctions, stay with it and send for any needed help. Correct the malfunction and verify that no classified pages remain in the machine.

4. All copies of classified documents reproduced for any authorized purpose are subject to the same controls prescribed for the document from which the reproduction is made.

5. HHS Form 208 must show the number and distribution of reproduced copies of all Top Secret and Secret documents, and any Confidential documents that bear special dissemination and reproduction limitations.

6-00-20 Protecting Controlled Unclassified Information

Sensitive But Unclassified (SBU) and For Official Use Only (FOUO) information is not classified national security information; therefore, it is not covered under the *Classified National Security Information Directive No. 1*, but they are covered by the legislation at large of the FOIA and the exceptions therein, as well as additional departmental and OPDIV/STAFFDIV guidance. The information, which usually involves sensitive Department activities, should be tightly controlled and stored.

Sensitive information should not be left in public view. If the level of access control within a facility is sufficient to preclude those without a need-to-know from accessing an individual's office or laboratory space, information may be left out in the open unattended. Otherwise the information should be locked in an office or a locking storage device, or be under the personal control of an authorized individual. No security clearance is required to handle SBU or FOUO information. Contact appropriate OPDIV/STAFFDIV records management officer for additional guidance on SBU and FOUO information.

U.S. Department of Health and Human Services

Subject: Storage

7-00-00 Purpose

This chapter provides instructions relating to the storage of classified information in accordance with the *Classified National Security Information Directive No. 1,* Subpart D.

7-00-05 Policy

Classified information must be stored under conditions designed to deter and detect unauthorized access to the information. Whenever classified information is not under the personal control and observation of a cleared employee who has been authorized access to information based on a need-to-know, the information must be stored in a locked security container approved for such storage.

7-00-10 Standards

The General Services Administration (GSA) establishes and publishes uniform standards, specifications, and supply schedules for security containers, vault door and frame units, and key operated and combination padlocks suitable for the storage and protection of classified information. Safe-type filing cabinets conforming to federal specifications bear a Test Certification Label on the locking drawer attesting to the security capabilities of the container and lock.

The Director, OSDT, may establish additional supplementary controls to prevent unauthorized access. The imposition of such additional controls should be based on the volume, nature, and sensitivity of the information to be protected in relation to

other factors, such as types of containers, presence of guards, vault-type space, and intrusion detection alarms.

7-00-15 Storage of Top Secret Information

When not in use, Top Secret information must be stored by one of the following methods and be inspected, certified, and approved by the Director, OSDT:

Table 10. Methods For The Storage Of Top Secret Information

METHODS FOR THE STORAGE OF TOP SECRET INFORMATION
• In a GSA-approved security container with one of the following supplemental controls: continuous protection by cleared guard or duty personnel; protected by an Intrusion Detection System (IDS) with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; in a security container that is inspected every two hours by cleared guard or duty personnel; or Security-In-Depth conditions, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.
• In an open storage area constructed in compliance with Section 4.1 of EO 12958, as amended, and protected by an IDS with the personnel responding to the alarms within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth or a five minute alarm response if it is not.
• An IDS-equipped vault with the personnel responding to the alarms within 15 minutes of the alarm annunciation.

The facility used for storage must be certified and approved by the Director, OSDT. Approval notice will be provided in writing to the OPDIV or STAFFDIV Head and/or CSO.

7-00-20 Storage of Secret Information

When not in use, Secret information is to be stored by one of the following methods:

Table 11. Methods For The Storage of Secret Information

METHODS FOR THE STORAGE OF SECRET INFORMATION
• In the same manner as with Top Secret information; or
• In a GSA-approved security container or vault without supplemental controls; or

METHODS FOR THE STORAGE OF SECRET INFORMATION
• In either of the following: A. Until October 1, 2012, in a non-GSA-approved* container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an OSDT or CSO approved padlock; B. Or an open storage area. For either method, one of the following supplemental controls is required: - The location that houses the container or open storage area is to be subject to continuous protection by a cleared guard or duty personnel; - Cleared guard or duty personnel is to inspect the security container or open storage area once every four hours; or - An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

*As part of the supplemental controls for a non-GSA-approved container or open storage area storing Secret information, a Security-in-Depth as determined by the Director, OSDT.

7-00-25 Storage of Confidential Information

Confidential information will be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

7-00-30 Combinations to Security Containers

The combination of a lock used for the storage of classified information is to be afforded protection equal to that given to the highest level of classified information stored in the container. Combinations to dial-type locks are to be changed only by personnel having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected, such as PSRs, CSO, LCOs, and Custodians of Classified Files, unless other sufficient controls exist to prevent access to the lock or knowledge of the combination.

The following are conditions when changing combinations is acceptable:

Table 12. Condition When to Change Combinations

CONDITIONS WHEN TO CHANGE COMBINATIONS
• When the container is placed in use; • When an employee knowing the combination no longer requires access to the combination; or • When a combination has been subject to possible compromise.

When security equipment is taken out of service, it is to be inspected to ensure that no classified information remains and the built-in combination lock is reset to a standard combination.

Combinations must be memorized, recorded on *Security Container Information* (SF 700), and stored in another approved security container. CSOs must establish procedures for the secure storage of the SF 700 combination envelope.

An SF 700 must be completed to show the names, addresses, and telephone numbers of personnel who are to be contacted if the security container, to which the form pertains, is found open and unattended by an authorized person. Part 1 of the form must be attached to the inside of the container so it is visible if the container is open.

Parts 2 and 2A of the SF 700 are used to record the security container's combination, which is inserted into the envelope portion for secure storage. Parts 2 and 2A of each completed copy of SF 700 must be classified at the highest level of classification of the information in the security container. A new SF 700 must be completed each time the combination to the security container is changed.

Access to the combination should be limited only to those employees who are cleared and have authorized access to the classified information stored in the container. Knowledge of combination must be limited to the minimum number of personnel necessary for operating purposes.

In accordance with Section 4.1 of EO 12958, as amended, when special circumstances exist, the Director, OSDT, may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks are to be established and approved by the Director, OSDT.

7-00-35 Relocation of Security Storage Containers

When an office having custody of classified information physically moves from one office or building to another, the classified information may be retained in the approved security container. However, the custodian, or other cleared employees, must maintain constant supervision of the container during the move. The CSO must be notified prior to relocating a security container used for the storage of classified information and may decide to store the classified information temporarily in another approved container.

7-00-40 Restrictions on Use of Storage Containers

Security containers used for the storage of classified information are not to be routinely used for the storage of cash, checks, weapons, controlled drugs, precious metals, personal items, or other items susceptible to theft.

Security storage containers should be located in an office occupied by a CSO, LCO, or Custodian of Classified Files, but must not be located in office storage areas, corridors, hallways, or in the vicinity of unsupervised exits.

7-00-45 Safe or Cabinet Security Record

An SF 702, *Security Container Check Sheet*, must be placed on the outside of each container holding classified information to record each time the container is opened and closed. The person opening and closing the container must write in the time of each operation and initial the form. There is also space on the SF 702 for the initials of the person performing the daily check for closure of the container. Someone must perform this check at the end of each work day to assure the container is locked. Each SF 702 can be used for four months and should be destroyed whenever a new one is placed in use.

SF 701, *Activity Security Checklist*, also can be used to provide additional assurance that security containers have been locked and other day-end security measures have occurred This form must be used in a security office or other locations where there are a number of security containers holding a large quantity of national security information.

U.S. Department of Health and Human Services

Subject: Transmission

8-00-00 Purpose

The purpose of this chapter is to provide instructions governing the transmission of classified information.

8-00-05 Transmittal Outside HHS Facility

All classified information transmitted outside a HHS building must be enclosed in opaque inner and outer covers (e.g., sealed envelopes or wrappings). Classified information must be addressed to a cleared individual with a security clearance commensurate with the highest level of classification of the information being transmitted. The inner cover will display the identity and forwarding address of the recipient, the return address, markings, and warning notices to indicate the highest security classification of the contents. The outer, sealed cover will only display the identity and forwarding address of the recipient and the return address.

Material used for packaging must be strong and durable to provide protection in transit and to prevent items from breaking out of the covers. Bulky packages must be sealed with tape laminated with asphalt and containing rayon fibers or nylon filament tape, or equivalent.

8-00-10 Transmittal Within HHS Facility or Facility Complex

All Sensitive Compartmented Information (SCI) classified information transmitted between offices within a HHS building or complex of buildings should be placed in a sealed opaque cover marked with the appropriate level of classification. All documents must have cover sheets attached (e.g., SF 703, 704, or 705). Classified information transmitted using these cover sheets must be promptly hand-delivered

by employees possessing a security clearance commensurate with the highest level of classification of the information.

Whenever security mail is opened in error by employees not authorized to open such mail, the envelope or container must be immediately resealed and marked "OPENED IN ERROR" (time and date) by (employee's name), and then promptly hand-carried to the proper recipient or LCP. In any such circumstances, it is the responsibility of the employee to ensure that the envelope or container is properly stored in the manner prescribed by Chapter 7-00 until personal delivery can be accomplished.

8-00-15 Receipt For Classified Information

HHS Form 25, *Classified Document Receipt*, must be completed for all transmissions of Top Secret and Secret information. The receipt shall be attached to or enclosed in the inner cover. The sender must retain his/her returned copy signed by the recipient as proof of the official transfer of the document(s): Top Secret receipts have a five-year retention period, and two years for Secret. The transmission of confidential information does not require a receipt, but may be used for further accountability.

8-00-20 Accountability Procedures Prior to Transmission

All classified material designated for transmission, regardless of designation, must be processed through the LCP, to include the TSCO if the information is Top Secret. The LCO must ensure that document accountability is maintained on HHS Form 208, that required receipts are attached and correct, and that the packaging meets requirements in Section 8-00-05.

8-00-25 Methods of Transmission

Top Secret level information must only be transmitted by one of the following methods and never via the United States Postal Service (USPS):

Table 13. Methods For Transmitting Top Secret Information

METHODS FOR TRANSMITTING TOP SECRET INFORMATION	
• Direct contact between authorized persons, hand-carried by designated employee (courier) with Top Secret	• The Defense Courrier Service; or • Diplomatic pouch through the Department of State Diplomatic Courier

METHODS FOR TRANSMITTING TOP SECRET INFORMATION	
clearance; • Cryptographic systems (e.g., automated information systems, secure telephone, secure facsimile systems) approved for the transmission of classified material at the appropriate level by the Director, National Security Agency (NSA), and authorized by the Director, OSDT;	System.

Secret level information must only be transmitted by one of the following methods and the use of external (street-side) collection boxes is prohibited:

Table 14. Primary Markings of Original Classification

METHODS FOR TRANSMITTING SECRET INFORMATION	
• Any of the means approved for the transmission of Top Secret information, except that the courier only needs to be cleared at the Secret level; • USPS Express Mail and USPS Registered Mail within and between the United States and its territories, as long as the Waiver of Signature and Indemnity block on the USPS Express Mail label is not completed; • USPS Registered Mail through Military Postal Service facilities for transmitting Secret level information to a US Government facility located outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a US possession or trust territory provided that the information does not at any time pass out of the control of the US citizen and does not pass through a foreign postal system or any foreign inspection;	• A cleared and designated employee (courier) on scheduled commercial passenger aircraft within and between the United States and its territories subject to the procedures and restrictions set forth in Section 8-OO-30; • Through cleared commercial carriers or cleared commercial messenger services; • Information classified up to Secret may be transmitted by an HHS messenger, provided the classified document is in a double envelope, as specified in Section 8-00-05 above, and handled like US registered mail with a receipt attached to the outer envelope; or • Agency heads may, on an exceptional basis and when an urgent requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the GSA contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations are met.

Confidential level information must only be transmitted by one of the following methods and the use of external (street-side) collection boxes is prohibited:

Table 15.Methods For Transmitting Confidential Information

METHODS FOR TRANSMITTING CONFIDENTIAL INFORMATION	
• Any of the means approved for the transmission of Top Secret or Secret information; or	• US First Class Mail when the recipient is a US Government facility. Ensure the envelope or outer wrapper is marked to indicate that the information is not to be forwarded, but is to be returned to the sender;

8-00-30 Carrying Classified Information By Couriers

The LCO shall authorize, orally or in writing, the use of the designated employee as a courier and assure the employee has been briefed in courier responsibilities as detailed in this chapter. Designated employees (couriers) may hand-carry classified information outside of HHS buildings subject to the following conditions:

Table 16. Restrictions Carrying Classified Information By Couriers

Restrictions Carrying Classified Information By Couriers	
• The employee's security clearance must be the same or higher than the classification of the material being carried; • The storage provisions of Chapter 7-00 apply at all stops en route to the destination, unless the information is retained in the personal possession and constant surveillance of the employee at all times. The hand-carrying of classified information on trips that involve an overnight stopover is not permissible without advance arrangements for proper overnight storage in a Federal Government installation or a cleared United States	• When classified information is carried in a private, public, or Government conveyance, it must not be left in automobiles, hotel rooms, hotel safes, aircraft or train compartments, private residence, or public lockers; • Employees must carry their HHS identification card or badge whenever carrying classified information outside of HHS buildings; • The LCO must be informed each time classified information is to be carried by an employee so that the LCO can designate that employee as a courier.

Restrictions Carrying Classified Information By Couriers	
contractor's facility;	

8-00-35 Aboard Commercial Passenger Aircraft

Classified information may be hand-carried aboard commercial passenger aircraft within and between the United States and its territories only in an emergency when the information is not available at the destination, and because of an urgent situation, there is neither time nor means available to transmit the information properly by the other methods stated in Section 8-00-25. Permission to hand-carry classified information aboard such aircraft shall be granted on a case-by-case basis by the Director, OSDT. Under no circumstances will any level of classified information be hand-carried across international boundaries.

Procedures for hand-carrying classified information aboard commercial passenger aircraft is as follows:

Table 17. Procedures For Hand-Carrying Classified Information Aboard Commercial Passenger Aircrafts

Procedures For Hand-Carrying Classified Information Aboard Commercial Passenger Aircrafts	
• This person will strictly comply with all provision of Section 8-00-30. • The person authorized to hand-carry the classified information will process through the routine airline ticketing and boarding procedures. The briefcase or carry-on luggage will be routinely offered for opening for inspection, if requested. • The screening officials may check envelope by x-ray machine, flexing, feel and weight, without opening the sealed envelope. Airport screening officials may be shown proper identification and the courier authorization documentation to avoid having the envelope opened.	• The person hand-carrying the classified information will be designated as a courier, in writing, by the Director, OSDT. • The classified information being hand-carried will not contain metal binding, it will be double-wrapped, addressed, and sealed as outlined in Section 8-00-05. The envelope will be placed in a briefcase or other piece of carry-on luggage. • If airline screening officials still insist on opening the envelope, the courier will ask to see a Federal Aviation Administration (FAA) field office representative. If the FAA

Procedures For Hand-Carrying Classified Information Aboard Commercial Passenger Aircrafts	
	representative still insists on opening the envelope after being shown proper identification and the courier authorization documentation, the courier will not attempt further boarding, but instead is to make alternate arrangements for completing the travel. Under no circumstances should the courier allow the envelope to be opened.

U.S. Department of Health and Human Services

Subject: Disposal and Destruction

9-00-00 Purpose

The purpose of this chapter is to provide instructions governing the disposal and destruction of classified information.

9-00-05 Disposal of Classified Information

Early disposal/destruction of unnecessary classified information can assist in preventing security violations, reducing security costs, and providing better protection for classified information that needs to be retained for some official purpose.

Some of the HHS classified holdings are non-permanent or non-record classified information, such as copies of classified documents from other agencies intended solely for reference purposes, as well as originally classified documents. These documents should be destroyed as soon as they have served their official intended purpose, have been superseded, or are obsolete. Retain those classified documents that contain current policy information. Other documentary record materials that are classified must be disposed of in accordance with General Records Schedule published by the National Achieves and Records Administration.

If HHS destroys information classified by another agency, the originating agency will likely have a copy if a copy is later needed for review. Proper documentation in the accountability records, HHS Form 208, will allow for tracking the document back to the originating agency.

9-00-10 Destruction of Classified Information

Documents containing classified information must be destroyed in a manner to preclude recognition or reconstruction of the classified information in whole or in part. Heads of offices or organizations (e.g., division directors) in possession of classified information must establish internal procedures for the proper destruction of classified information. Such procedures must ensure that adequate destruction methods are used, classified information is protected during transport to the

destruction area, adequate records are maintained, and the destruction is properly witnessed.

Destruction of classified information must be accomplished by one of the following methods and the methods of destruction and the equipment used for such must be approved by the CSO:

Table 18. Methods For The Destruction Of Classified Material

Methods For The Destruction of Classified Material	
• Cross-cut shredders may be used for the destruction of classified information provided the shredders are listed on the GSA Federal Supply Schedule as approved security destruction devices. These approved shredders cross-cut the strips to a size of approximately l/32" in width and l/2'& in length. • Burning, when approved by the CSO, may be used for the destruction of classified information. The documents containing the information must be burned completely and no unburned pieces shall remain or be allowed to escape by wind or draft.	• Additional methods include wet-pulping, disintegration, chemical decomposition, mutilation, or pulverization.

Classified material awaiting destruction must be properly stored in an approved security storage container. Boxes, bags, sealed envelopes, or other like containers used for the collection and transportation of classified material must provide adequate safeguards to prevent the loss of the material. When transporting classified material to a destruction area, such containers must not be left unattended.

The lower portion of HHS Form 25 is the official Certificate of Destruction and must be used as a receipt to indicate the destruction of Top Secret and Secret information. The form must include a full unclassified description of the material, the date of actual destruction, and witness to the actual destruction. For Top Secret information, two employees must sign the form, one as the destruction official and the other as the witnessing official. Just the destruction official is required to sign for Secret information. Employees who conduct and witness the destruction of classified information must possess a security clearance commensurate with highest

level of information being destroyed. Destruction certificates are not required for Confidential information unless prescribed by the agency that originated the information.

HHS Form 25, used for the destruction of Secret or Confidential information, must be maintained for a minimum of two years. When used for the destruction of Top Secret information, the form must be maintained for five years and then destroyed. These destruction certificates can be maintained at any location approved by the CSO.

Classified waste material must be destroyed as soon as practical by one of the approved destruction methods. This applies to all waste material containing classified information, such as preliminary drafts, carbon sheets, fabrics or plastic typewriter ribbons, diskettes, stencils, stenographic notes, working papers, and similar items. Employees who are designated to destroy classified waste material must possess the appropriate security clearance and the need-to-know the information. Destruction certificates are not required for classified waste material. Pending destruction, all classified waste material must be stored in an approved security container.

Classified messages, which are generated during a classified exercise, need not be processed into an accountability system or brought under control if they are destroyed within 30 calendar days after completion of the exercise. Certificates of destruction are not required for these messages. However, classified exercise messages that are retained beyond the 30-day period will be controlled and destroyed in the same manner as other accountable classified messages. These classified messages, awaiting destruction, must be safeguarded and stored in the manner stated in Chapter 7-00.

9-00-15 Emergency Protection, Removal, and Destruction

In the event of fire, natural disaster, civil disturbance, or an evacuation of office space, classified information must be protected either by placing it in a locked, approved security container, relocating it to another office/organization for proper storage, or by properly destroying the information. Employees who are away from their office and have classified information in their possession at the time of an emergency must assure that such information is properly safeguarded or destroyed.

Only the Secretary or designee may order the safe removal or emergency destruction of US and NATO classified material. Upon receipt of the order, the Director, OSDT, will immediately notify the LCOs of all affected offices and inform them of the emergency plan. In all situations, highest priority for removal or

destruction will be given to the highest level of classified material (i.e., Top Secret Special Access is first priority, then regular Top Secret, then NATO Secret, then regular Secret, etc.).

The CSO must ensure that all offices in possession of classified information must have plans for the emergency protection, removal, and destruction of the information. The location and identity of the information to be destroyed, priorities for destruction, persons responsible for destruction, and recommended place and

method of destruction must be predetermined and persons fully indoctrinated. The Director, OSDT, can assist in the preparation of such plans.

A copy of the written plans for emergency handling of classified information should be filed in a readily accessible location inside each security container being used for the storage of classified information.

U.S. Department of Health and Human Services

Subject: Security Awareness, Contact With Certain Foreign Nationals, And Foreign Travel

10-00-00 Purpose

This chapter provides PSRs and employees with instructions relating to security awareness concerns regarding contact with certain foreign nationals and specific foreign travel requirements in accordance with the *Reporting Hostile Contacts and Security Awareness* NSDD-197.

10-00-05 Security Awareness And Reporting Contact With Certain Foreign Nationals

The *Reporting Hostile Contacts and Security Awareness* NSDD-197 sets the standards for the Department's security education and training programs. HHS maintains a formalized security awareness program designed to ensure that employees are aware of the potential threat to the Department's classified, proprietary, and sensitive information from foreign sources, whether overt or covert. This program must include an initial and refresher training, periodic formal briefing of the threat posed by hostile intelligence services, and termination briefings. The program must provide for the practices and reporting, under defined circumstances, of the employee contacts with nationals of certain designated foreign countries or political entities.

HHS employees who, through their job functions or access to national security or sensitive information or technology, become targets for exploitation by foreign intelligence services and HHS employees have the requirement to report such incidents. HHS personnel (employees and contractors) with security clearances are to be briefed, at least once a year, on foreign travel security procedures by their corresponding OPDIV or STAFFDIV PSR. The unauthorized release of sensitive

information or technology and contacts with foreign nationals of high risk designated countries must be reported in accordance with the provisions of this Section. These HHS employees have certain reporting requirements. They must report all contacts with individuals of any nationality, either within or outside the scope of the their official activities, in which:

1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

2. They are concerned that they may be the target of an attempted exploitation by a foreign entity.

These employees must also report all contacts with nationals of high-risk, designated countries (see Section 10-00-15), which appear to indicate an attempt or intention to obtain unauthorized access to classified, proprietary, or sensitive information; offer a reasonable potential for such access; or indicate the possibility of continued professional or personal contacts.

Employees subject to these reporting requirements must submit a written report to the PSR within five days of the occurrence. Employees in doubt as to whether a written report is required should call their PSR or the Director, OSDT. The report should be as specific as possible regarding the facts about the contact, including the identity of the hostile or potentially hostile source. The PSR must promptly notify the Director, OSDT, about the employee's report and the Director, OSDT, will notify the FBI, if deemed necessary.

Table 19. Definitions Of Certain Security Words and Terms

Definitions of Certain Security Words and Terms	
Contact	Means any form of meeting, association, or communication regardless of who initiated the contact or whether it was for social, official, or private purposes. This includes any contact in person, by telephone, letter, radio, or any form of communication, even if no official information was discussed or requested.
Proprietary Information	Business information which was developed by the private sector and furnished to the Department with the expectation or condition that it be protected. Information of this type, referred to as trade secret material, requires protection against unauthorized disclosure under Title 18, U.S.C., Section 1905 and Title 21, U.S.C., Section 3315.

Definitions of Certain Security Words and Terms	
Sensitive Information	Unclassified information, which if lost, exploited, or disclosed without authority, could impair the national security or foreign relations of the US, or affect the ability of the Department to meet stated goals and/or objectives of national interest. Sensitive information also includes that privileged information which qualifies as an exemption under the Freedom of Information and the Privacy Act of 1974, and other information provided by another US Department or Agency with the expectation or condition that the information will be protected. "Sensitive" information does not include information in the public domain or that given out under the auspices of bilateral agreements.

None of the reporting requirements contained in this chapter are intended to replace existing agreements between the Department of State and HHS components to report suspicious activities. These requirements are in addition to those already established. Employees with SCI access have additional reporting requirements (See Section 10-00-10 below).

10-00-10 Foreign Travel Requirements

HHS employees who travel to foreign countries to attend international, scientific, technical, medical, or other professional meetings or conferences may come into contact with representatives of high-risk designated countries.

All HHS personnel (employees and contractors) who intend to travel to non-NATO countries are to notify the appropriated OPDIV or STAFFDIV PSR in advance of such trip. At the discretion of the OPDIV or STAFFDIV PSR, a pre-travel briefing and post-travel debriefing may be required in connection with travel to a non-NATO country.

Travel to designated countries by HHS personnel (employees and contractors) must to be approved in advance by the Director, OSDT. All HHS personnel (employees and contractors) who intend to travel to designated countries or events where nationals of designated countries can reasonably be expected to be in attendance, shall, at the discretion of the OPDIV or STAFFDIV PSR, receive a pre-travel briefing and a post-travel debriefing.

HHS employees, who have Top Secret clearances with SCI access, must report to the Director, OSDT, their intent to travel to foreign countries for non-official purposes. They must report this information, orally or in writing, in advance of the planned trip, whether on private or official business, so that they can be afforded a

defensive security briefing. Other HHS employees may request such a briefing from their PSR, who can obtain briefing materials from the Director, OSDT.

This defensive security briefing is in addition to any normal Department of State briefing provided to government employees traveling on official business. The briefing will cover safeguarding requirements for classified and other sensitive information and will include security awareness guidelines.

When any employee with SCI access returns from personal foreign travel, he/she must contact the Director, OSDT, for a security debriefing. Other employees traveling to these designated countries should report any incidents or concerns to their PSR. The employees should be advised that it is essential to report any suspected attempts to obtain classified, proprietary, or sensitive information, or efforts to recruit, compromise, harass, or entrap the employee. Such information received by a PSR must be promptly reported to the Director, OSDT.

HHS employees traveling overseas to perform extended temporary duty (TDY), defined as more than 30 days at an overseas location, are required to take the Department of State's Foreign Service Institute's approved mandatory training or equivalent security training provided by their corresponding PSR.

10-00-15 Designated Countries

The current list of the designated high-risk countries, for which there are reporting and travel requirements, can be obtained from PSRs or OSDT.

10-00-20 NATO Countries

These are the NATO members as of the date of issuance of this manual:

Table 20. NATO Countries

NATO Countries	
Belgium	Lithuania
Bulgaria	Luxembourg
Canada	Netherlands
Czech Republic	Norway
Denmark	Poland

NATO Countries	
Estonia	Portugal
France	Romania
Germany	Slovakia
Greece	Slovenia
Hungary	Spain
Iceland	Turkey
Italy	United Kingdom
Latvia	United States

10-00-25 Foreign Visitors

OPDIV and STAFFDIV heads will ensure that an HHS employee ("HHS Hosting Official") is assigned in advanced to every foreign national who visits an HHS facility. The HHS Hosting Official will be responsible for ensuring that the foreign national's visit is in full compliance with applicable policies and procedures. The HHS Hosting Official will inform the OPDIV or STAFFDIV PSR seven working days in advance of any visit to such OPDIV or STAFFDIV by a foreign national.

OPDIV and STAFFDIV heads will ensure that foreign nationals do not have unsupervised access to Critical Infrastructure sites. Critical Infrastructure is defined as systems and assets so vital to the mission of HHS that the incapacity or destruction of such site would have a debilitating impact on the nation's security, economy or public health. The OPDIV or STAFFDIV PSR may grant exceptions to this policy. The HHS Hosting Official will obtain approval from the OPDIV or STAFFDIV PSR prior to any visit by a foreign national to any HHS laboratory or other facility designated as Critical Infrastructure. Exceptions for nationals of high-risk designated countries must be approved by the Director, OSDT. The HHS Hosting Official will inform the Director, OSDT, five working days for approval from the Director, OSDT prior to any visit by a national of a non-NATO country to any HHS facility designated as Critical Infrastructure.

U.S. Department of Health and Human Services

Subject: Other Special Security Programs

11-00-00 Purpose

The purpose of this chapter is to provide general information and instructions regarding other special security programs that could be of interest to some Department officials who have national security responsibilities.

11-00-05 Policy

It shall be the policy of the Department to establish, where an identifiable need exists, the special security programs described in this chapter and to comply fully with security directives issued by the Federal agencies identified for each program area.

11-00-10 COMSEC and Secure Voice

COMSEC means protective measures taken to deny unauthorized persons information derived from telecommunications or to assure its authenticity. Such protection results from the application of various security measures, including crypto-security, transmission and emission security, and certain physical security measures needed for protection of COMSEC information and materials. The National Manager, National Security Telecommunications and Information Systems Security Committee (NSTISSC), is responsible for issuing COMSEC instructions for all approved cryptographic systems.

National security information must not be discussed over, or otherwise transmitted or processed by, any form of telecommunications unless approved measures are taken to protect the information. COMSEC is the only system of security measures used to protect classified information utilizing cryptographic keying material and equipment.

The Secure Telephone Units (STU) III and the Secure Telecommunication Equipment (STE) developed by the NSA provide, by use of COMSEC measures, secure voice transmission capability during discussions involving the highest levels

of classified national security information and other highly sensitive/proprietary information.

The COMSEC Custodian is responsible for implementing NSTISSC guidance in the OPDIV and STAFFDIV.

Upon determining the need for any COMSEC support or secure voice transmission system capability, the PSR should submit a request to the Director, OSDT. The request shall contain all pertinent circumstances relating to the type of support or system needed.

Specific cryptographic access requirements are required for some HHS employees, such as COMSEC Custodians, because of their on-going need to handle certain classified cryptographic information. The Director, OSDT, is responsible for processing and issuing cryptographic accesses that meet the policy requirements of the National Telecommunications and Information Systems Security Committee.

11-00-15 North Atlantic Treaty Organization

The US national security authority responsible for the security of NATO classified information is USSAN. The USSAN is the Secretary of Defense. The USSAN has established, under the Secretary of the Army, a US national registry known as the Central United States Registry (CUSR). The Chief, CUSR, is authorized to establish and disestablish US NATO subregistries, release NATO documents to US departments and agencies, and conduct inspections of all subregistries and control points.

NATO security procedures governing the protection and handling of NATO classified information in the possession of this Department are contained in USSAN Instruction l-69, *Implementation of NATO Security Procedures*. The instruction, which contains some NATO classified information, has been assigned an overall classification of CONFIDENTIAL.

A NATO SECRET subregistry, established in accordance with USSAN Instruction l-69, is located in the Office of the Director, OSDT. The Director, OSDT, is authorized to establish NATO SECRET Control Points where an operational need exists to maintain certain NATO SECRET, CONFIDENTIAL, or RESTRICTED information.

Written justification relating to the need of a control point shall include a description of the classified NATO documents needed and be furnished to the Director, OSDT. Formal access to NATO classified information may be authorized only when the

Department has authorized an employee access to US information of an equivalent classification and the employee has been given a NATO security briefing.

11-00-20 Special Access Programs

A Special Access Program is a program that imposes "need-to-know" or access controls beyond those normally provided for access to Top Secret, Secret, or Confidential information. Such a program includes, but is not limited to, special clearance, investigative and adjudication requirements, special designation of officials authorized to determine "need-to-know," and special classified lists of persons granted SCI clearance.

Special Access Programs are created only by a Federal agency that possesses original classification authority. The programs are compartmentalized to further restrict access to those who "need-to-know" certain national security information. The Director, OSDT, is responsible for processing all requests for access to Special Access Programs and assuring that special security requirements are met.

U.S. Department of Health and Human Services

Subject: Industrial Security

12-00-00 Purpose

The purpose of this chapter is to provide policies and procedures for HHS in participation in NISP. OSDT administers the Department's Industrial Security Program. OSDT establishes policies and implements procedures to ensure the appropriate safeguarding of classified and sensitive unclassified information which is released to or generated by prime contractors, subcontractors or self employed individuals under contract to the Department. This includes all private sector individuals supporting Department activities either assigned at HHS locations or performing on contracts from their companies' respective physical locations.

12-00-05 Authority

The NISP was established by E.O. 12829 on January 6, 1993. EO 12829, as amended, provides for the protection of classified information in accordance with *Classified National Security Information Directive No. 1*.

12-00-10 Applicability

NISP was created to provide for uniform and standardized policies and procedures for all Federal agencies, departments, and contractors. The Secretary of Defense has been designated Executive Agent for the NISP by the President. The NISPOM gives practical application to these objectives by serving as the single regulatory standard for the NISP and serving as the sole national guidance for HHS' Industrial Security Program. The suitability of contractors is considered to be the same as that of an HHS employee; only those company contractors needing security

clearances are covered by NISP. In accordance with the NISP, DoD is responsible for conducting, and adjudicating the background investigations, making the security determinations, and granting security clearances to contractor companies and their employees.

12-00-15 The Cognizant Security Agency and Office

The term "Cognizant Security Agency" (CSA) denotes the DoD, the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency. The Secretary of Defense, the Secretary of Energy, the Director of Central Intelligence and the Chairman, Nuclear Regulatory Commission may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more "Cognizant Security Offices."

The Cognizant Security Offices is the office or offices delegated by the Head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA. It is the obligation of each CSA to inform industry of the applicable Cognizant Security Office. The Cognizant Security Office is responsible for executing *Security Agreements* Form (DD Form 441) with contractors on behalf of the Government; conducts security surveys and inspections of HHS contractor facilities; grants facility and personnel clearances to HHS contractors; investigates the loss or compromise of classified HHS information in the hands of contractors, and serves as the primary point of contact on all security matters between the Government and the contractor.

The CSA for HHS is the Department of Defense and the CSO for HHS is the Defense Security Service.

12-00-20 The Defense Security Service (DSS)

DSS administers the NISP on behalf of DoD and non-DoD Federal agencies within the Executive Branch of the Government. Under the NISP, DSS Industrial Security Representatives oversee cleared contractor facilities and assist the organizations' management staff and Facility Security Officers in formulating their security programs. DSS inspects and monitors contractors who require or will require access to classified information and provides oversight, advice and assistance to contractor facilities that are cleared for access to classified information under the NISP.

The Office of Security and Drug Testing will be the principal contact with DSS and, within the OPDIVs/STAFFDIVs, the servicing PSR will be the HHS interface for matters regarding Industrial Security and will coordinate with DoD to provide security clearances for company contractors working for their organization.

12-00-25 Facility Security Clearances (FCL)

All contractors, experts, and consultants employed by a company who have a need to use, process, store, reproduce, transmit, transport, or handle classified information at any location in connection with HHS-related activities will require a facility clearance. This specifically includes situations where a contractor, expert, and consultant needs to have access to HHS classified information in relation to their HHS regulated activities.

Also included are others who require access to classified information in connection with HHS regulated activities but do not require use, storage, or possession of classified information outside of HHS facilities. An HHS component needs to sponsor a contractor for the clearance and the request will be addressed to DSS, Defense Industrial Security Clearance Office (DISCO), Facility Clearance Division.

The eligibility requirements to be processed for a FCL include that the contractor's company must have a reputation for integrity and lawful conduct in its business dealings; it must be organized and existing under the laws of any of the fifty states, the District of Columbia, or Puerto Rico, and be located in the U.S. or its territorial areas or possessions; and must not be under foreign ownership, control, or influence to a such a degree that the granting of the FCL would be inconsistent with the national interest.

If necessary, DSS will make the accreditation decision on the facility in which classified information is to be housed, stored or generated. A determination based on review and approval of a Standard Practice Procedures Plan to grant a facility clearance will be conducted. This review includes a finding that the facility is not under foreign ownership, control, or influence to such a degree that a determination could not be made.

12-00-30 Background Investigations for a Security Clearance for Contractors and Consultants

All contractors, experts, and consultants who are employed by a company and who require routine and continuing access to HHS owned and leased facilities and are part of a contract requiring access to national security information in order to

perform work for HHS, are required to have a security clearance granted by DoD. The requirement of the background security investigation must be included in the formal government contract. A *Classification Specification Form* (DD Form 254) must be incorporated in each classified contract. DD Form 254 provides the security requirements and the classification guidance to the contractor, which would be necessary to perform on a classified contract. The servicing PSR will coordinate the submission of DD Form 254 to DSS and provide a copy to OSDT.

Individuals who do not work for a company and are without a sponsoring private organization, yet still require access to national security information per the scope of their work for HHS or direct employment contracts with HHS, are required to have a suitability determination conducted and follow the same policies and procedures as Federal employees to obtain a security clearance. Individuals working as consultants without a sponsoring private organization will be cleared by OSDT as if they are employees.

12-00-35 Clearances Verification

The servicing PSR will obtain security clearance verification of contractors, experts, and consultants and ensure that the individuals have been granted the appropriate level of security clearance and have a bonafide “need-to-know” for the information in the performance of their duties prior to granting access to HHS facilities where classified information will be disclosed. As is done for Federal employees, specific types of investigation are conducted for each of the different types of security clearance need by a contractor, expert, or consultant in the performance of official work for HHS.

12-00-40 National Interest Determination (NID)

A company cleared under a Special Security Agreement (SSA) with its cleared employees may only be afforded access to "proscribed information" with special authorization. This special authorization must be manifested by a favorable NID that must be program/project/contract-specific. Access to proscribed information must be predicated on a decision by the Deputy Secretary of HHS that release of such information to a company cleared under the SSA arrangement will not harm the national security interests of the United States. The servicing PSR will prepare the proposed NID and send it to OSDT which will review it on behalf of the Deputy Secretary of HHS and then forward it to the Deputy Secretary for approval and submission to DSS headquarters.

12-00-45 Arranging and Processing a Request for a Classified Visit

Arrangements through the servicing PSR are to be made for visits in which classified material is to be handled, processed, or discussed. These should be made sufficiently in advance to permit expeditious processing. Verification of security clearances for contractors, experts, and consultants may be passed to the servicing PSR by the Security Office of any contractor, expert, or consultant cleared under the DoD Industrial Security Program.

All contractors, experts, and consultants must comply with the policies and procedures of the NISPOM and those of this manual. When a clearance is no longer required for job performance, the HHS will administratively withdraw a security clearance via the servicing PSR and the sponsoring private organization's security personnel.

APPENDIX A - Terms And Definitions

TERMS AND DEFINITIONS	
Access	The ability and opportunity to obtain knowledge of classified national security information.
Agency	A Federal agency as defined in Title 5 U.S.C., Section 552(e).
Classification Security Officer (CSO)	An OPDIV or STAFFDIV official who is responsible for providing guidance and oversight to their organization on the control and safeguarding of classified National Security Information. It is also the responsibility of this official to conduct an initial classification review of documents created by their organization and coordinate this review with Office of Security and Drug Testing. This official is to keep current information on their organizations LCOs and LCPs.
Compromise	The known or suspected exposure of classified information to an unauthorized person.
CONFIDENTIAL	It is applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.
Controlled Area	Any area, entry to which is subject to restrictions for security reasons.
Custodian of Classified Files	An employee who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.
Declassification	A determination, made by an original classification authority, that classified information no longer requires, in the interests of national security, protection against unauthorized disclosure under EO 12958, as amended, together with a removal or cancellation of the classification designation.
Derivative Classification	A determination that information is in substance the same as information currently classified. The newly developed information is marked consistent with the classified markings of the source material.
Downgrade	A determination made by the originating authority that particular classified information requires, in the interests of the national security, a lower degree of protection than currently provided. This determination requires changing of the classification designation to reflect such lower degree of protection.

TERMS AND DEFINITIONS

Inadvertent Access	An incident in which an employee had access to classified information to which the employee was not authorized.
Logging Control Officer (LCO)	An employee responsible for the proper maintenance of records relating to the safeguarding and storage, accountability, transmission and destruction of national security information.
Logging Control Point (LCP)	A central place within an office or organization where all classified information received, recorded, stored, transmitted or destroyed.
Multiple Sources	The term used to indicate that a document that is derivatively classified contains classified information derived from more than one source.
National Industrial Security Program	The National Industrial Security Program ("NISP"), was established to safeguard classified information held by contractors, licensees, and grantees of the United States Government in a cost effective and efficient manner.
National Security	The national defense and/or critical foreign relations of the United States
National Security Information	Information that has been determined pursuant to EO 12958, as amended, or any predecessor EO concerning national security, to require protection against unauthorized disclosure. National security information is also referred to as classified information. Such information must be appropriately marked TOP SECRET, SECRET, or CONFIDENTIAL, according to contents, by an official possessing the original classification authority under EO 12958, as amended .
Original Classification	An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.
Original Classification Authority (OCA)	The authority vested in a designated Executive Branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. HHS has been granted this authority.
Personnel Security Representative (PSR)	A Senior management official designated, in writing, the responsibility for his/her organization's personnel security program. PSRs maintain lists of those individuals within their organization who have security clearances.

TERMS AND DEFINITIONS

Security Classification Levels	National Security Information is classified at the three TOP SECRET, SECRET, or CONFIDENTIAL levels.
SECRET	It is applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.
Security Clearance	An administrative determination based upon the results of a favorably adjudicated investigation that an individual is trustworthy and may be granted access to a specified level of national security information as required in the performance of assigned duties (see HHS Instruction 731-I for clearance procedures).
Special Access	That special compartmented category of national security information accessible to selected individuals on a must know basis. It requires a current Top Secret clearance, a recent Special Background Investigation (SBI), specific justification to the agency responsible for the special access program, and a unique security briefing.
TOP SECRET	It is applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.
TOP SECRET Control Account	An approved method within an established LCP for the storage, receipt, and transmission of Top Secret documents, when authorized in accordance with section I-00-30C
TOP SECRET Control Officer (TSCO)	An official who has a Top Secret clearance and is designated in writing to be responsible for receiving, safeguarding, controlling, accounting for, and destroying all Top Secret documents within the TSCO's assigned area of responsibility.
Unauthorized Disclosure	A communication or physical transfer of specific classified information to a person not authorized access to that level of classified information or not having met need-to-know requirements.

APPENDIX B - ACRONYMS

ACRONYMS	
CDC	Centers for Disease Control and Prevention
COMSEC	Communications Security
CSA	Cognizant Security Agency
CSO	Classification Security Officer
DD Form 254	*Classification Specification Form*
DD Form 441	*Security Agreements* Form
DHS	Department of Homeland Security
DISCO	Defense Industrial Security Clearance Office
DOE	Department of Energy
DoD	Department of Defense
DSS	Defense Security Service
EO	Executive Order
FAA	Federal Aviation Administration
FCL	Facility Security Clearances
FDA	Food and Drug Administration
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GSA	General Services Administration
HHS	Health and Human Services
HHS Form 25	Classified Document Receipt
HHS Form 207	Request for Security Clearance Form
HHS Form 208	Classified Document Accountability Record
IDS	Intrusion Detection System
ISCAP	Interagency Security Classification Appeals Panel

ACRONYMS

ISOO	Information Security Oversight Office
LCO	Logging Control Officer
LCP	Logging Control Point
NATO	North Atlantic Treaty Organization
NID	National Interest Determination
NIH	National Institutes of Health
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NSA	National Security Agency
NSDD	National Security Decision Directive
NSDD-84	Safeguarding National Security Information
NSDD-197	Reporting Hostile Contacts and Security Awareness
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTISSP	National Telecommunications and Information Systems Security Policy
OCA	Original Classification Authority
OPDIV	Operating Division
OSDT	Office of Security and Drug Testing
PA	Privacy Act
PDD	Presidential Decision Directive
PSR	Personnel Security Representative
RFP	Request for Proposal
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF 312	Classified Information Nondisclosure Agreement Standard Form

ACRONYMS

SF 700	Security Container Information
SF 701	Activity Security Checklist
SF 702	Security Container Check Sheet
SF 703	Top Secret Cover Sheet
SF 704	Secret Cover Sheet
SF 705	Confidential Cover Sheet
SSA	Special Security Agreement
STAFFDIV	Staff Divisions
STE	Secure Telecommunication Equipment
STU	Secure Telephone Units
TDY	Extended temporary duty
TSCO	Top Secret Control Officer
U.S.C.	United States Code
USPS	United States Postal Service
USSAN	U.S. Security Authority for North Atlantic Treaty Organization Affairs