Department of Homeland Security
Management Directive System
MD Number: 11045

Issue Date: 10/04/2004

PROTECTION OF CLASSIFIED NATIONAL SECURITY INFORMATION: ACCOUNTABILITY, CONTROL, AND STORAGE

1. Purpose

This directive implements Executive Order 12958, as amended, Classified National Security Information. It prescribes the safeguarding requirements of the classified national security information program within the Department of Homeland Security (DHS).

2. Scope

This directive is applicable to all persons who are permanently or temporarily assigned, attached, detailed to, or under contract with, DHS. It is also applicable to other officials outside the Federal government that have been provided access to classified information.

3. Authority

A. Executive Order 12333, United States Intelligence Activities.

B. Executive Order 12829, National Industrial Security Program.

C. Executive Order 12958, as amended, Classified National Security Information.

D. Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security.

E. 6 CFR, Part 7, Department of Homeland Security, Classified National Security Information.

F. 32 CFR, Part 2001/2004, Implementing Directive for EO 12958, as amended.

G. 44 U.S.C. Chapters 21, 31 and 33, Federal Records Act.

H. PL 96-456, Classified Information Procedures Act.

I. National Telecommunications Information Systems Security Instruction (NTISSI) C-4004.

J. Federal Standard 89, Neutralization and Repair of GSA Approved Containers.

K. CNSS Policy No. 16, National Policy for the Destruction of COMSEC Paper Material.

L. DHS Management Directive 0010.1, Management Directives System and DHS Announcements and Enclosures.

M. DHS Management Directive 11046, Requirements for Open Storage Areas.

4. Definitions

A. ***Authorized Person:*** A person who has a need-to-know for access to classified information in the performance of official duties and who has been granted a personnel clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an authorized person rests with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient.

B. ***Classification:*** The act or process by which information is determined to be classified information.

C. ***Classified National Security Information ("Classified Information"):*** Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

D. ***COMSEC:*** The communications security systems, services, and concepts that constitute protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of any /such communications.

E. ***Confidential:*** A level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

F. ***Derivative Classification:*** The incorporating, paraphrasing, restating, or generating, in a new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes classification of information based on guidance provided in a security classification guide. The duplication or reproduction of existing classified information is not derivative classification.

G. ***Information:*** Any knowledge that can be communicated or is documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

H. ***Information Security:*** As used in this directive, information security is the system of policies, procedures, and requirements established under the authority of Executive Order 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. Information security is commonly referred to as INFOSEC.

I. ***Need-to-Know:*** A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

J. ***Organizational Element (OE):*** As used in this directive, organizational element is as defined in DHS MD Number 0010.1, "Management Directive System and DHS Announcements."

K. ***Original Classification Authority:*** An individual authorized in writing, either by the President, or by agency heads, or other officials designated by the President, to classify information in the first instance.

L. ***Secret:*** Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

M. ***Security Liaison:*** An official who is assigned responsibility for implementing and managing an organizational element's security program as a secondary or additional duty.

N. ***Security Officer:*** Authorized position within an organizational element whose primary duties are to serve as the lead official for developing, implementing, and managing security programs within the organizational element.

O. ***Senior Agency Official:*** The official designated by the agency head under section 5.4(d) of E.O. 12958, as amended, who directs and administers the agency's program under which information is classified, safeguarded, and declassified. The Senior Agency Official for DHS is the Chief Security Officer.

P. ***Top Secret:*** Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

5. Responsibilities

A. The Secretary of Homeland Security has designated the Chief Security Officer (CSO) as the Senior Agency Official (SAO). The Senior Agency Official shall:

1. Direct and administer the Department's program under which information is classified, safeguarded, and declassified.

2. Coordinate the Department's classification management program and serve as the DHS point of contact on matters associated with the Information Security Oversight Office (ISOO).

3. Promulgate and publish implementing directives as necessary for program implementation and ensure procedures are established and implemented to prevent unauthorized and unnecessary access to classified information.

4. Promulgate implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public.

5. Establish and maintain security education and training programs.

6. Establish and maintain a self-inspection and periodic review program to review and assess the management and safeguarding of classified information created and/or possessed by DHS agencies.

7. Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas.

8. Ensure the performance contract, or other system used to rate civilian or military personnel performance, includes the management of classified information as a critical element to be evaluated in the rating of:

   a. Original Classification Authorities;

   b. Security Managers, security specialists, or other officials performing security functions involving the safeguarding of classified information; and

   c. Other personnel whose duties involve the creation or handling of classified information.

9. Account for costs associated with the implementation of programs for the protection of classified information. Report such costs to the Information Security Oversight Office (ISOO) upon request.

10. Assign promptly, personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of Executive Order 12958, as amended, that pertains to classified information that originated in an organizational element of DHS that no longer exists and for which there is no clear successor in function.

11. Report violations, take corrective measures, and assess appropriate sanctions as warranted, in accordance with Executive Order 12958, as amended.

12. Oversee DHS participation in special access programs authorized under Executive Order 12958, as amended.

13. Establish procedures to prevent unnecessary access to classified information, including procedures that:

a. Require that a need for access to classified information is established before initiating administrative clearance procedures; and

b. Ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

14. Perform any other management duties as required by the position of SAO that the Secretary may designate.

B. The Chief, Administrative Security Division, shall under the direction and authority of the SAO/CSO, administer, manage, and provide oversight for all programs relating to the safeguarding of classified information, as cited in this directive.

C. The Heads of Organizational Elements shall:

1. Ensure sufficient resources are in place to implement and manage the Information Security Program and the requirements of this directive.

2. Appoint a senior official within the organizational element to serve as the organizational element Security Officer/Security Liaison.

3. Issue additional written procedures, as necessary, for the effective implementation of this directive. Procedures written to augment or supplement this directive may exceed the requirements cited in this directive but shall not lessen them. Where an organizational element chooses to exceed the standards as cited herein, sufficient justification must exist to warrant any increased expenditures.

D. The OE Security Officer/Security Liaison shall:

1. Serve as the advisor to the head of the OE for all matters relating to implementing and complying with the provisions of this directive.

2. On behalf of the head of the OE, implement, monitor, manage, and oversee the provisions of this directive within his/her respective OE.

3. Act as liaison between the OE, DHS headquarters security staff, and other security officials both inside and outside of government.

4. Implement a viable and robust security education and training program within their respective organizations.

E. Supervisors and Managers shall:

1. Ensure they are aware of, and comply with, the applicable provisions of this directive, and promote and ensure compliance by staff members.

2. Begin security education and awareness upon initial assignment of an employee and reinforce periodically thereafter through routine office interaction, e-mail reminders, staff meetings, and other office gatherings, or any other method or media contributing to an informed workforce.

F. All DHS personnel shall be:

1. Responsible for protecting classified information from unauthorized disclosure.

2. Aware of and comply with the applicable provisions of this directive, and report to appropriate officials, infractions, or violations that affect the safeguarding of classified information.

6. Policy & Procedures

A. Policy.

1. This directive prescribes the minimum standards for the protection of classified information. Organizational elements may exceed the standards cited in this directive but may not lessen them. Where an organizational element chooses to exceed the standards as cited herein, sufficient justification must exist to warrant any increased expenditures.

2. Requests to waive requirements as cited in this directive will be submitted through the Security Officer/Security Liaison of the requesting organizational element to the DHS Chief Security Officer. Waiver requests must include sufficient justification to support the request and identification of compensatory measures that will be implemented to mitigate deficiencies.

B. Procedures.

1. Accountability and Control. DHS Organizational Elements shall have a system of control measures that ensure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons. The following are minimum administrative control measures:

a. Top Secret

1) Top Secret Control Officer (TSCO): Each program office that routinely handles or stores TOP SECRET information will appoint a primary TSCO and as many alternates as are necessary to manage the TOP SECRET Control Account (TSCA). Officials appointed as TSCO or Alternate TSCO will possess a final Top Secret security clearance. The TSCO will maintain records for the accountability, dissemination, and destruction of TOP SECRET information. All TOP SECRET information will be processed (incoming and outgoing) to and through the TSCO.

2) Top Secret Document Register: A TOP SECRET Document Register will be maintained by the TSCO to record the receipt, disposition, and destruction of TOP SECRET information. DHS Form 11000-03, Document Control Register, Top Secret National Security Information, may be used for this purpose. Other forms or automated registers created by an organizational element may also be used, but, at a minimum, must contain the information included in DHS Form 11000-03. Electronic registers must be backed up after each transaction to ensure no loss of accountability.

3) Top Secret Control Number: Each TOP SECRET document entered into the TSCA will be assigned a document control number (DCN). The DCN will consist of the office identifier, or other coding information, indicating the specific office possessing the document, the calendar year, and a sequential number indicating the number of documents generated/received within the calendar year. For example, EP&R/NSC 03-04 when translated is: EP&R, Office of National Security Coordination, calendar year 2003, and the 4th document entered into the TSCA for that calendar year.

4) Top Secret Signature Record: Each TOP SECRET document in the TSCA will have attached to it a TOP SECRET Signature Record, DHS Form 11000-04. Each person having access to the TOP SECRET information will sign and date the form indicating they had access.

5) Top Secret Inventories: No later than December 31 of each year, a hands-on inventory of TOP SECRET materials maintained in a TSCA will be conducted. The inventory will be conducted by an official other than the TSCO or alternate TSCO. The inventory official will be appointed by the head of the office where the TSCA is maintained. Upon completion of the inventory, a written report will be completed conveying the results of the inventory to the head of the applicable office. Discrepancies cited during the conduct of the inventory will be investigated and reconciled. A copy of the inventory reports will be maintained by the TSCO until the next inventory is completed.

b. Secret and Confidential: Except as required by the originator or as specified for certain categories of SECRET and CONFIDENTIAL information, there is no requirement to maintain accountability records or conduct inventories for SECRET and/or CONFIDENTIAL information. However, heads of organizational elements may mandate the use of accountability records within their respective elements at their discretion.

c. Receipts: Organizational elements shall implement procedures to ensure timely completion of receipt for TOP SECRET and SECRET materials transmitted or transferred outside an organizational element. DHS Form 11000-11, Document Record of Transmittal, or a similar transmittal form, may be used for this purpose. With the exception of certain categories of information, e.g., NATO and foreign government information, and materials transmitted to a cleared contractor, receipts for CONFIDENTIAL materials will be at the discretion of the sender.

C. Access

1. Access to classified information shall be limited to persons whose official duties require knowledge or possession of the information. No one has a right to have access to classified information solely by virtue of office, rank, or position. Three criteria shall be met prior to granting access:

a. Security Clearance. The intended recipient has been granted a security clearance equal to or higher than the level of classified information to which access will be granted.

b. Need-to-know. The intended recipient has a need-to-know the information in the performance of official governmental duties. The responsibility for determining whether an individual possesses the need-to-know for access to classified information rests with the authorized holder of the information. Where the authorized holder of the information is uncertain as to an intended recipient's need-to-know, they should contact an official in their supervisory chain or the originator of the classified information.

c. Where access involves the physical transfer of classified materials from one cleared person to another, the intended recipient has the means to properly store the materials.

2. Third Agency Rule: Classified information originated by another government agency and furnished to a DHS organizational element shall not be further distributed outside DHS without the prior consent of the originating agency. Unless limitations have been imposed by the originator, this restriction does not apply to further distribution within and between organizational elements of DHS, or distribution to cleared contractors who require the information in the performance of a DHS contract.

3. Access by Persons Outside of the Executive Branch: Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the U.S. Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DHS organizational elements shall designate appropriate officials to determine, before the release of classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know.

a. Judicial: DHS Office of the General Counsel will be consulted whenever a litigation request or demand is made upon DHS personnel for official DHS information or for testimony concerning such information. The personnel upon whom the request or demand was made shall immediately notify the servicing DHS legal office. Classified information entered into the Judicial System shall be handled in accordance with the Classified Information Procedures Act (PL 96-456). Justices of the U.S. Supreme Court and Judges of the U.S. Courts of Appeals and District Courts do not require an investigation and determination of eligibility for access to classified information. All other members of the Judiciary must be appropriately investigated and granted a security clearance.

b. Congress: Access to classified information or material by Congress, its committees, members, and staff representatives shall be coordinated through the DHS Office of Legislative Affairs. Any DHS

employee testifying before a Congressional committee in executive session, in relation to a classified matter, shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of information that may be discussed. Members of Congress, by virtue of their elected positions, do not require an investigation and determination of eligibility for access to classified information. All other congressional staff members and other associated officials must be appropriately investigated and granted a security clearance. (The Office of the Inspector General is exempt from this requirement when acting in their official capacity.)

c. State, Local, Tribal, and Private Sector Officials: State Governors, by virtue of their elected positions, do not require an investigation and determination for eligibility for access to collateral classified information. Other State, Local, Tribal, and Private Sector Officials must be appropriately investigated and granted a security clearance by DHS or other Federal government agencies.

d. Government Printing Office (GPO): Documents and material of all classification may be processed by the GPO, which protects the information in accordance with the guidelines outlined in EO 12958, as amended.

e. Representatives of the Government Accountability Office (GAO): Representatives of the GAO may be granted access to classified information when such information is relevant to the performance of the statutory responsibilities of that office. Certifications of security clearances, and the basis thereof, shall be accomplished pursuant to arrangements between GAO and the DHS organizational element concerned.

f. Historical Researchers: Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that a DHS Original Classification Authority (OCA), with classification jurisdiction over the information, accomplishes the following:

1) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted, and certifies that the requester has been found to be trustworthy based on such investigation as determined by the CSO.

2) Limits such access to specific categories of information over which the DHS organizational element has classification jurisdiction, and to any other category of information for which the

researcher obtains the written consent of a DHS organizational element OCA, or non-DHS Department or Agency that has classification jurisdiction over information contained in or revealed by the document, within the scope of the proposed historical research.

3) Maintains custody of the classified material at a DHS installation or activity, or authorizes access to documents in the custody of the National Archives and Records Administration.

4) Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscripts for review by DHS organizational elements or non-DHS departments or agencies with classification jurisdiction, for a determination that no classified information is contained therein. This information shall be included in a non-disclosure agreement, which shall be executed by the researcher as a condition of access.

5) Issues an authorization for access valid for not more than two years from the date of issuance.

g. Former Presidential Appointees: Persons who previously occupied policy-making positions to which the President appointed them, may not remove classified information upon departure from office. Such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, upon approval of the Secretary, Deputy Secretary or Chief Security Officer in consultation with the Office of the General Counsel. The approving official shall:

1) Make a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted, and by certifying that the requester has been determined to be trustworthy based on such investigation as determined by the CSO.

2) Limit access to specific categories of information over which DHS has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a non-DHS Department or Agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed access.

3) Retain custody of the classified material at a DHS installation or activity, or authorizes access to documents in the custody of the

National Archives and Records Administration.

4) Obtain the former presidential appointee's agreement, through the execution of a non-disclosure agreement, to safeguard the information and to submit any notes and manuscripts for review by DHS or non-DHS departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

h. Visit Notifications. Heads of DHS organizational elements shall establish procedures to accommodate visits to their facilities involving access to, or disclosure of, classified information. At a minimum, these procedures will include verification of the identity, personnel security clearance, access, and need-to-know for all visitors. Visits by officials such as members of Congress, or by GAO, will be coordinated through the appropriate office. Visit requests (security clearance verification) shall be submitted by the Security Office of the parent organization to the DHS visit sponsor. Visit requests hand-carried by a visitor shall not be honored or accepted.

i. Emergency Situations. In an emergency, and when necessary to respond to an imminent threat to life or in defense of the homeland, the Secretary, Deputy Secretary, Under Secretary for Infrastructure Protection and Information Analysis, Under Secretary for Emergency Preparedness and Response, Under Secretary for Border and Transportation Security, Assistant Secretary for Information Analysis, Assistant Secretary for Infrastructure Protection, the DHS Chief Security Officer, Director, Homeland Security Operations Center, Director, Integration Staff, Commandant, U.S. Coast Guard, Assistant Commandant for Intelligence, U.S. Coast Guard, Director, U.S. Secret Service, and the Special Agent in Charge, Intelligence Division, U.S. Secret Service, may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Under these conditions, the approving official shall:

1) Limit the amount of classified information disclosed and the number of individuals to whom it is disclosed to the absolute minimum necessary to achieve the intended purpose;

2) Transmit the classified information via approved Federal Government channels by the most secure and expeditious method possible, or by other means deemed necessary when time is of the essence;

3) Provide instructions about what specific information is classified and how it should be safeguarded. Physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary and unique of circumstances;

4) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement. In emergency situations requiring immediate verbal release of information, the signed nondisclosure agreement memorializing the briefing may be received after the emergency abates;

5) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than seven days after the release, the disclosing authority shall notify the DHS CSO and the originating agency of the information. Such notification shall include:

a) A description of the disclosed information;

b) To whom the information was disclosed;

c) How the information was disclosed and transmitted;

d) Reason for the emergency release;

e) How the information is being safeguarded; and

f) A description of the briefings provided and a copy of the nondisclosure agreements signed.

6) A copy of the signed nondisclosure agreements should be forwarded with the notification referenced in paragraph 5, above, or as soon thereafter as practical.

7) Release of information pursuant to this authority does not constitute declassification thereof.

8) This authority may not be further delegated.

D. Safeguarding. Personnel who have been granted access to classified information are responsible for protecting the information in their possession or control, and must ensure proper precautions are taken to prevent unauthorized access. Classified information must be protected at all times either by storage in an approved container or facility, or having it under the personal observation and control of an

authorized individual.

1. Care During Working Hours. Items containing classified information, such as preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter and printer ribbons, electronic media, and other items, shall be either destroyed immediately after they have served their purpose or protected as required for the level of classified information they contain. Any media containing classified information, in any form, shall be appropriately secured when unattended.

2. Cover Sheets. Classified information removed from storage shall be kept under constant surveillance by authorized personnel. Standard Forms 703, 704, and 705, classified document cover sheets, will be placed on classified documents when not in secure storage containers.

3. End-of-Day Security Checks. Activities that process or store classified information shall establish and implement a system of security checks at the close of each working day to ensure that the area is secure and classified information has been properly stored. Standard Form 701, "Activity Security Checklist," shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for the storage of classified material; Standard Form 702, "Security Container Check Sheet," shall be used to record such actions. In addition, Standard Forms 701 and 702 shall be annotated to reflect after-hours, weekend, and holiday activity.

4. Emergency Planning.

a. Plans shall be developed for protecting, removing or destroying classified information in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action to minimize the risk of compromise. The level of detail and amount of testing and rehearsal of these plans should be determined by an assessment of the risk of hostile action, natural disaster or terrorist activity that might place the information in jeopardy.

b. Planning for the emergency protection (including emergency destruction under no-notice conditions) of classified COMSEC material shall be developed in accordance with the requirements of National Telecommunications Information Systems Security Instruction (NTISSI) C-4004. When preparing emergency plans, consideration should be given to reducing classified material on hand by destroying unneeded material, retiring unneeded material, or transferring unneeded material to automated information systems media.

5. Telephone Conversations. Classified information shall not be discussed telephonically except over approved and encrypted equipment.

6. Removal of Classified Storage Equipment. Storage containers used to store classified information shall be inspected by properly cleared personnel prior to removal from protected areas, or before unauthorized persons are allowed access to them. The inspection should ensure that no classified information remains in the container. Organizational elements shall establish procedures to ensure equipment is thoroughly inspected.

7. Residential Storage

a. Only the Secretary, Deputy Secretary, or DHS Chief Security Officer may authorize the storage of classified information in private residences. Requests for in-residence storage of classified information shall be submitted, with justification, to the DHS Chief Security Officer.

b. When residential storage is approved, a GSA-approved security container shall be furnished. For storage of Top Secret information, an intrusion detection alarm system meeting UL standards shall also be in place and operational. Written procedures shall be developed to provide for appropriate protection of the information, to include a record of the information that is authorized for residential storage. These procedures will be coordinated through the DHS Chief Security Officer.

8. Classified Meetings and Conferences. Meetings and conferences that involve classified information present special vulnerabilities to unauthorized disclosure. Heads of DHS organizational elements, or their designees, shall establish specific requirements for protecting classified information at conferences, seminars, exhibits, symposia, conventions, training courses, or other such gatherings where classified information is disseminated. For in-house gatherings and other impromptu meetings, see paragraph 9, below. At a minimum, the following shall apply:

a. The meeting will serve a specific U.S. Government purpose;

b. The use of other appropriate channels for dissemination of classified information or material are insufficient;

c. The meeting location will be under the security control of a U.S. Government Agency, or a U.S. contractor with an appropriate facility security clearance;

d. Adequate security procedures have been developed and will be implemented to minimize risk to the classified information involved (refer to procedures cited in paragraph 9, below);

e. Classified sessions shall be segregated from unclassified sessions whenever possible;

f. Access to the meeting or conference, or specific sessions thereof, at which classified information will be discussed or disseminated, will be limited to persons who possess an appropriate security clearance and need-to-know;

g. Announcement of the classified meeting shall be unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions. Non-government organizations may assist in organizing and providing administrative support for a classified meeting, but all security requirements remain the specific responsibility of the DHS organizational element sponsoring the meeting. Procedures must ensure that classified documents, recordings, audiovisual material, magnetic media, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by other provisions of this Directive. Note taking or electronic recording during classified sessions shall be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting.

h. The DHS organizational element sponsoring the meeting should appoint a DHS official to serve as security manager for the meeting. The physical security of the actual site of the classified meeting is established and maintained by U.S. Government personnel.

i. Other U.S. Government organizations, or cleared DHS contractors with appropriate facility security clearances, may assist with implementing security requirements under the direction of the appointed security manager.

9. For in-house gatherings and other impromptu meetings where classified information will be discussed, it is incumbent upon the host or sponsor of the meeting to ensure appropriate security measures are in place. Those measures shall include:

a. The meeting is held in an area under the security control of a U.S. Government agency, or at an appropriately cleared U.S. contractor facility.

b. Ensuring that all electronic equipment maintained in the room capable of transmitting signals outside the room, is powered off and disconnected from electrical outlets.

c. Conduct a sound attenuation test to ensure normal conversational tone from inside the room cannot be heard intelligibly from outside the room – pay particular attention to vents, ducts, and other openings. If public address or other amplification systems are used, conduct the test with these systems on and off.

d. Assign and post cleared host office personnel at exterior doors and hallways to keep the room's perimeter under surveillance and prevent passers-by from stopping and listening.

e. Control access to the room. Use an attendee roster if applicable, and have sufficient backup host office personnel available, as needed.

f. Verify the identity of each participant via U.S. Government photo-identification or similar documentation.

g. Ensure the security clearances of attendees are at least equal to the level of classified information to be disclosed.

h. Prohibit those without proper authorization and clearance from attending classified portions of the meeting.

i. Notify each attendee and presenter of:

1) The highest level of classified information to be presented/discussed and when multiple presentations are given, the specific classification (or unclassified status) of each presentation.

2) Limits on the number of room entrances and the access controls prior to or during the meeting to prevent access by unauthorized persons.

3) Limitations associated with classified portions of the meeting, e.g., prohibitions against photographing, note-taking, audio/video recording, using two-way radios, cellular phones, or other transmitting devices.

j. Ensure security protection for the room is maintained during breaks.

k. Comply with all security safeguards for classified information.

l. At the conclusion of the meeting, conduct an inspection of the room to ensure no classified materials have been left behind.

m. If applicable, ensure sufficient supplies are available to properly package classified materials for local attendees to hand-carry back to their office. For those outside the local area, gather, package, and mail classified materials to the attendees' office.

10. U.S. Classified Information Located in Foreign Countries. Except for classified information that has been authorized for release to a foreign government, U.S. classified material may be retained in foreign countries only when necessary to satisfy specific U.S. Government requirements. Heads of the DHS organizational elements will prescribe requirements for protection of this information, with particular attention to ensuring proper enforcement of controls or release of classified information to foreign entities. Classified material in foreign countries shall be stored:

a. At a U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. At a U.S. Government entity located in a building used exclusively by U.S. Government tenants, provided the building is under 24-hour control by U.S. Government personnel.

c. At a U.S. government entity located in a building not used exclusively by U.S. Government tenants, or under host government control, provided the classified material is stored in security containers approved by the GSA and under 24-hour control by U.S. Government personnel.

d. At a U.S. Government entity located in a building not used exclusively by U.S. Government tenants, but that is under host government control, provided the classified material is stored in GSA-approved security containers that are further secured in a locked room or area to which only U.S. personnel have access.

11. Computer Equipment and Removable Storage Media.

The Department of Homeland Security has a variety of non-COMSEC-approved equipment used to process classified information. This includes copiers, facsimile machines, computer equipment and peripherals, electronic typewriters, word processing systems, and others. Organizational elements shall identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Organizational element security procedures shall prescribe the appropriate safeguards to:

a. Prevent unauthorized access to the equipment and/or information.

b. Replace and destroy equipment parts as classified material when the information cannot be removed from them or protected appropriately, commensurate with the level of classification.

c. Ensure that appropriately cleared and technically knowledgeable personnel inspect equipment before the equipment is removed from protected areas.

d. Classified Information will not be processed on any equipment unless it has been certified and accredited for classified processing (refer to DHS Policy Publication 4300B, DHS National Security Systems Handbook).

E. Storage. Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this directive represent acceptable security standards. Weapons or sensitive items such as funds, jewels, precious metals, or drugs shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence through various Director of Central Intelligence Directives (DCIDs). Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

1. Standards for Storage Equipment. GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

2. New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms shall conform to Federal Specification FF-L-2740. Existing non-FF-L-2740 mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF-L-2740 standards.

3. Maintenance performed on GSA-approved containers must be in accordance with Federal Standard 89, Neutralization and Repair of GSA-Approved Containers. When repairs to a GSA-approved container affect its original integrity, the GSA-approved label shall be removed and the container will no longer be authorized for the storage of classified information.

4. Storage of Classified Information. Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area, as follows:

a. Top Secret

1) Top Secret information shall be stored in a GSA-approved security container. One or more of the following supplemental controls must also be in place:

a) The location that houses the security container is subject to continuous protection by cleared guard or duty personnel;

b) Cleared guard or duty personnel inspect the security container once every two hours;

c) An Intrusion Detection System (IDS) is in place with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or

d) Security-In-Depth, as determined by the organizational element Security Official, when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.

e) Modular vault, vault, or a secure room constructed in accordance with guidance issued by DHS Office of Security and equipped with an IDS, with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a 5-minute alarm response time if it is not. (Other rooms that were approved for the storage of Top Secret in the U.S. may continue to be used.)

b. Secret. Secret information shall be stored by one of the following methods:

1) In the same manner as prescribed for TOP SECRET information;

2) In a GSA-approved security container or vault without supplemental controls;

3) In a secure room that is approved for the open storage of SECRET information;

4) 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 lock bar and a GSA-approved padlock. When stored in a non-GSA-approved container, one or more of the following supplemental controls must be in place:

a) The location that houses the container is subject to continuous protection by cleared guard or duty personnel;

b) Cleared guard or duty personnel shall inspect the security container once every four hours; or

c) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm.

c. Confidential. CONFIDENTIAL information shall be stored in the same manner as prescribed for TOP SECRET or SECRET information except that supplemental controls are not required.

d. Open Storage. Approval of open storage will be considered when the volume of materials or operational necessity of the mission dictates. The organizational element's security official must authorize approval, in writing, for a space or office to be designated for the open storage of classified information. Refer to DHS Management Directive 11046 on Open Storage.

e. Equipment Designations. There shall be no external mark revealing the level of classified information authorized to be, or actually stored in, a given container or vault, or to the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol, (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes).

f. Combinations to Containers and Vaults

1) Only persons having an appropriate security clearance and need-to-know shall change combinations to security containers, vaults, and secure rooms used for the storage of classified information.

2) The combination of a container, vault, or secure room used for the storage of classified information shall be treated as information having a classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the appropriate classification level. Standard Form 700, Security Container Information, will be used for this purpose.

3) Combinations shall be changed:

a) When placed in use;

b) Whenever an individual knowing the combination no longer requires access to it, unless other sufficient controls exists to

prevent access to the lock;

c) When the combination has been subject to possible compromise;

d) When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

e) Every two years, if none of the above conditions have been applied.

f) GSA-approved field safes and special purpose one- and two-drawer, light-weight security containers, approved by the GSA, are used primarily for storage of classified information in the field. Such containers shall be securely fastened to a permanent structure or under sufficient surveillance to prevent their theft.

F. Reproduction of Classified Material. Documents and other materials containing classified information shall be reproduced only when necessary to accomplish the mission of the organization, or for compliance with applicable statutes or directives. Since reproduction equipment and the reproduction process involve substantial risk, DHS organizational elements shall establish and enforce procedures for reproduction of classified information that limit reproduction to that which is mission-essential and will ensure that appropriate countermeasures are taken to negate or minimize risk. The use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

1. Approval for Reproduction. Unless restricted by the originating agency, TOP SECRET, SECRET, and CONFIDENTIAL information may be reproduced to the extent required by operational needs. For accountability purposes, reproduction of TOP SECRET information will be coordinated through the TSCO. Organizational elements shall establish procedures that, at a minimum:

a. Ensure compliance with reproduction limitations placed on documents by originators and special controls applicable to Special Access Programs and other special categories of information;

b. Facilitate oversight and control of reproduction of classified material; and,

c. Ensure the expeditious processing of documents in connection with review for declassification.

2. Control Procedures. Organizational elements shall establish controls to ensure that:

a. Reproduction is kept to a minimum consistent with mission requirements;

b. Classified material is not reproduced on equipment that poses unacceptable risks, for example, machines that are connected to an unclassified LAN, equipped with remote diagnostics, equipped with an internal memory, or in some other way retain images;

c. Personnel doing the reproduction are aware of the risks involved with the specific reproduction equipment and the appropriate countermeasures they are required to take;

d. Reproduced material is clearly identified as classified at the applicable level;

e. Reproduced material is placed under the same accountability and control requirements as apply to the original material; and

f. Waste products generated during reproduction are properly protected and disposed of.

G. Disposition and Destruction of Classified Material

1. Classified documents and other materials shall be retained within DHS organizations only if they are required for effective and efficient operation of the organization, or if law or regulation requires their retention. Documents that are no longer required for operational purposes shall be disposed of in accordance with the provisions of the Federal Records Act and appropriate implementing directives and records schedules. Material that has been identified for destruction shall continue to be protected, as appropriate for its classification, until it is actually destroyed. Destruction of classified documents and materials shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

2. Organizational elements shall ensure that retention management of classified information is included in oversight and evaluation of program effectiveness. Each activity with classified holdings should establish at least one day each year when specific attention and effort is focused on disposition of unneeded classified material ("clean-out day").

3. Methods and Standards

a. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

b. Cross-cut shredders currently in use that produce a residue particle size that does not exceed 1/32 inch in width by ½ inch in length may continue to be used for the destruction of classified information. Where maintenance is performed on such machines that involves rebuilding the shredder blade assembly, or, where new shredders are purchased for the destruction of classified information, the replacement or new purchase shall comply with CNSS Policy No. 16, National Policy for the Destruction of COMSEC Paper Material, and be equipment listed on the National Security Agency (NSA) Evaluated Products List (EPL) of High Security Crosscut Shredders. A copy of the EPL can be obtained by calling the NSA National Information Assurance Center at (800) 688-6115. Technical guidance on other methods of destruction can be obtained by contacting the DHS Office of Security.

c. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755.

H. Alternative Control Measures

1. The DHS Chief Security Officer may approve the use of alternative security controls to ensure that the protection afforded classified information is sufficient to reasonably deter and detect actual or possible compromise. Approval to use alternative control measures shall be submitted to the DHS Chief, Administrative Security Division.

2. Alternative security control measures shall be employed only when the minimum standards in this directive cannot be met, and after considering risk management factors such as criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated, vulnerability to exploitation, and countermeasures benefits versus cost.

7. Questions

Questions regarding this management directive should be addressed to the Department of Homeland Security Office of Security.