Department of Homeland Security
Management Directive System
MD Number: 11041
Issue Date: 8/12/2004

PROTECTION OF CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM MANAGEMENT

I. Purpose

This directive implements Executive Order 12958, as amended, Classified National Security Information. It prescribes the program management, report, and oversight portions of the classified national security program within the Department of Homeland Security (DHS).

II. 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.

III. Authority

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

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

C. Executive Order 12333, United States Intelligence Activities.

D. Executive Order 12829, National Industrial Security Program.

E. 6 C.F.R., Part 7, Department of Homeland Security, Classified National Security Information.

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

IV. Definitions

A. ***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.

B. ***Information***: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, 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 the information, or its successor in function, to regulate access to the information.

C. ***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.

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

E. ***Security Liaison***: An official who is assigned responsibility for implementation and management of an organizational element's security program as a secondary or additional duty.

F. ***Security Officer***: Authorized position within an organizational element whose primary duties are to serve as the lead official for the development, implementation, and management of security programs within the organizational element.

V. Responsibilities

A. The Secretary of Homeland Security has designated the ***Chief Security Officer (CSO)*** as the ***Senior Agency Official (SAO)***. As the SAO, the CSO 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. Publish and promulgate 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 an ongoing self-inspection and periodic review program to 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 that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item 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;

   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, pursuant to E.O. 12958, as amended. Report such costs to the Information Security Oversight Office (ISOO) upon request.

10. Promptly assign 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 Senior Agency Official that the Secretary may designate.

15. Direct and administer the Department's Personnel Security Program in accordance with Executive Order 12968.

16. Direct and administer the Department's implementation and compliance with the National Industrial Security Program in accordance with Executive Order 12829.

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.

D. The organizational element ***Security Officer/Security Liaison*** shall:

1. Serve as the advisor to the head of the organizational element for all matters relating to implementation and compliance with the provisions of this directive;

2. Implement, monitor, manage, and oversee the provisions of this directive within his/her respective organizational element;

3. Act as liaison between the organizational element, organizational element counterparts, 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 in close coordination with the Office of Security.

E. ***Supervisors and Managers*** shall:

1. Ensure that they, and those that they supervise, 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, detailee, and contractor, and reinforce periodically thereafter through routine office interaction, e-mail reminders, staff meetings and other office gatherings, or any other method or media, which will contribute to an informed workforce.

F. All personnel shall:

1. Be responsible for protecting classified information from unauthorized disclosure;

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

VI. Policy & Procedures

A. ***General***.

1. Programs and safeguards established for the identification and safeguarding of classified information are necessary to ensure the integrity of U.S. national security and national interests. All personnel employed by or attached to DHS are personally and individually responsible for protecting classified information under their custody and control in accordance with the requirements set forth in this directive.

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

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

4. Nothing in this directive is intended to conflict with or circumscribe the authority of the Office of the Inspector General.

B. ***Reports***.

The following recurring reports are required to monitor and manage the efficiency and effectiveness of the Information Security Program:

1. SF 311

Standard Form (SF) 311, Agency Security Classification Management Program Data Report reflects the status of an agency's classification management program. Each organizational element will submit a single report reflecting the classification and declassification actions taken during the preceding fiscal year. The DHS Chief Security Officer will compile input from the organizational elements into a single DHS report for submission to the Information Security Oversight Office (ISOO). Organizational elements will submit the report upon request by the DHS Chief Security Officer.

2. Lock Replacement Report

32 CFR Parts 2001/2004, Section 2001.43, Classified National Security Information (Directive No. 1); Final Rule, requires the use of GSA Approved equipment for the storage of classified information. Further, locks used on equipment for the storage of classified information must meet Federal Specification FF-L-2740-A. The referenced directive allows agencies until October 1, 2012, to meet the referenced standards.

Organizational elements shall develop a plan to replace equipment used for the storage of classified information that does not meet the standards referenced above. Organizational elements shall report the status of their replacement plan to the DHS Office of Security upon request by the Chief Security Officer. This report is expected to coincide with the reporting requirement cited in VI.B.1 above.

3. Cost Accounting Report

This report will reflect the estimated costs expended for the protection of classified information for the current fiscal year, the previous fiscal year, and the next fiscal year. Reports will be submitted to the DHS Chief Security Officer. Each organizational element will submit a single report reflecting the estimated costs for all organizational elements within the respective organization. The DHS Chief Security Officer will compile input from the organizational elements into a single DHS report for submission to the Information Security Oversight Office (ISOO). Organizational elements will submit the report upon request by the DHS Chief Security Officer.

4. Report of Organizational Element Violations/Infractions

This report will consist of the total number of confirmed violations/infractions, by category, occurring within an organizational element in the preceding calendar year with the exception of incidents involving Communications Security (COMSEC) and Special Compartmented Information (SCI). COMSEC and SCI incidents are reported through other channels. Each organizational element will submit a single report reflecting the violations/infractions for all organizational elements within the respective organization. The report will be submitted to the DHS Chief Security Officer by January 15 of each calendar year, documenting confirmed violations/infractions for the preceding calendar year. The purpose of the report is to provide DHS-wide trend analysis for determining enhanced and focused educational and awareness needs.

C. ***Oversight & Compliance***.

1. DHS Office of Security

The Office of Security has overall responsibility for the oversight of and compliance with the standards set forth in this directive. As such, the Office of Security will conduct periodic program reviews of organizational elements to assess compliance and provide guidance and assistance as necessary.

2. Self-Inspections

Each DHS organizational element shall establish and maintain a self-inspection program based on program needs and the degree of involvement with classified information. The purpose of the program shall be to evaluate and assess the effectiveness and efficiency of the organization's implementation of the Information Security Program. Such assessments shall not conflict with, supersede, or substitute for Office of Inspector General assessments of such matters.

At a minimum, the self-inspection program shall include the conduct of a program review of each office that handles and/or stores classified information at least once per calendar year. A standard program review checklist is provided at Appendix 1. This checklist, or other locally developed tools, may be used to record program review results and follow-up actions.

Organizational elements shall ensure that deficiencies cited during the conduct of a self-inspection are appropriately resolved. A copy of the results of a self-inspection shall be retained for one year or until superseded by another self-inspection, whichever is later. A review of the previous self-inspection shall be conducted as part of any follow-up or follow-on self-inspections.

U.S. DEPARTMENT OF THE HOMELAND SECURITY
INFORMATION SECURITY REVIEW GUIDE

Conducted By:	
Program Office:	
Date:	

No.	Description	Yes	No	N/A
A	**Program Management**			
1	Has a Security Officer/Security Liaison been appointed in writing? Comment:			
2	Does the organizational element conduct annual internal Information Security self-inspections? Comment:			
3	Is a record of the results of internal Information Security self-inspections maintained? Comment:			
4	Has action been taken to eliminate deficiencies noted during the internal self-inspection? Comment:			
5	Is there evidence of an effective and viable Security Awareness Program? Comment:			
6	Are personnel aware of their responsibility to report known or suspected security incidents and/or violations? Comment:			

No.	Description	Yes	No	N/A
7	Are security incidents/violations reported promptly to the appropriate officials? Comment:			
B	**Classification Management**			
1	Are classification challenges encouraged when holders of information believe that the classification is improper? Comment:			
2	Are persons with classification responsibilities aware of the difference between original and derivative classification? Comment:			
3	Are persons aware of DHS original and derivative classification authorities? Comment:			
4	Have persons who exercise ***original*** classification authority been trained? Comment:			
5	Has the ***original*** classification authority prepared and published a security classification guide for the classification of program specific information? Comment:			

No.	Description	Yes	No	N/A
6	Document marking: Are ***originally*** classified documents appropriately marked to include: Overall Page markings Portion Markings "Classified By" Line (MUST be a designated Original Classifier) "Reason" Line "Declassify On" Line Comment:			
7	Do ***originally*** classified materials meet the standards for classification as set forth in Executive Order 12958, as amended? Comment:			
8	Have appropriate declassification instructions for ***originally*** classified materials been applied? Comment:			
9	Has the program office provided appropriate input regarding ***original*** classification decisions for the annual SF 311 Report, Agency Security Classification Management Program Data Report? Comment:			
10	Have persons who exercise ***derivative*** classification authority been trained? Comment:			

No.	Description	Yes	No	N/A
11	Document marking: Are ***derivatively*** classified documents appropriately marked to include: Overall Page Markings Portion Markings "Derived From" Line "Declassify On" Line Comment:			
12	Based on a random sampling of source and derived documents, do DHS created ***derivatively*** classified documents honor the classification markings cited on the source? Comment:			
13	Where "Multiple Sources" is cited as a "Derived From" line, is a record maintained with the file copy of what the multiple sources are? Comment:			
14	Has the program office provided appropriate input regarding ***derivative*** classification actions for the annual SF 311, Agency Security Classification Management Program Data Report? Comment:			
15	Is a record maintained of the number of originally classified and derivatively classified documents created? Comment:			
16	Are documents containing foreign government information properly marked? Comment:			

No.	Description	Yes	No	N/A
17	Are classified working papers properly marked and either destroyed or marked as a finished document when kept for more than 180 days, sent outside of the originating office, or filed permanently? Comment:			
C	**Document Security/Accountability**			
1	Prior to releasing or revealing DHS classified information to another Federal agency are the following verified: the security clearance of the intended recipient, need-to-know, and, if applicable, does the intended recipient have the proper means to store the materials? Comment:			
2	Prior to releasing or revealing information classified by another Federal agency to a third party Federal agency, is approval received from the originating agency? Are the following verified: the security clearance of the intended recipient, need-to-know, and, if applicable, does the intended recipient have the proper means to store the materials? Comment:			
3	Prior to releasing or revealing classified information to another DHS employee, are the following verified: the security clearance of the intended recipient, need-to-know, and, if applicable, does the intended recipient have the proper means to store the materials? Comment:			
4	Is classified information/material transmitted only by authorized means? Comment:			
5	Are personnel responsible for transmitting classified materials aware of the proper packaging and transmission procedures? Comment:			

No.	Description	Yes	No	N/A
6	Is accountable mail, i.e., Registered, USPS Express Mail, properly secured until its contents are determined? Comment:			
7	Are incoming accountable receipts for classified materials promptly signed and returned to sender? Comment:			
8	Is a DHS 11000-11, Classified Document Record of Transmittal, used when transmitting Top Secret, Secret and Confidential material? Comment:			
9	Are procedures established and followed to trace outgoing accountable mail receipts not returned to sender within twenty (20) business days? Comment:			
10	Are classified cover sheets used properly? Comment:			
11	Have persons who hand-carry classified materials outside of a DHS facility been briefed on the procedures for hand-carrying classified materials and been issued a courier authorization letter or card? Comment:			
12	Do persons with a need to hand-carry classified materials aboard commercial aircraft request prior approval? Comment:			

No.	Description	Yes	No	N/A
D	**Top Secret Control Account**			
1	Has a Top Secret Control Officer (TSCO) been appointed and does the TSCO possess a Top Secret security clearance? Comment:			
2	Is DHS Form 11000-03, Document Control Register – Top Secret National Security Information, used to maintain accountability of Top Secret materials in the account? Comment:			
3	Are DHS Top Secret Control Numbers properly assigned to Top Secret documents originated by or received into the TSCA? Comment:			
4	Are accountability records for Top Secret materials retained with the Top Secret Document Register? Comment:			
5	Has a DHS Form 11000-04, Top Secret Signature Record, been prepared and placed on top of each TS file, which all personnel viewing the file must endorse? Comment:			
6	Are Top Secret materials inventoried annually or upon change of a TSCO? Comment:			

No.	Description	Yes	No	N/A
7	Was the inventory conducted by an appropriately cleared, disinterested party, in conjunction with the TSCO? Comment:			
8	Is a record of the inventory results maintained? Comment:			
9	Are Top Secret materials appropriately stored and accessible only by persons possessing a Top Secret security clearance? Comment:			
E	**Safekeeping/Storage**			
1	Is access to classified containers limited to appropriately cleared personnel with a need to know? Comment:			
2	Where possible, are classified materials segregated from unclassified materials? Comment:			
3	Are funds, weapons, medical items, or other items of intrinsic value prohibited from being stored in the same container used for storage of classified information? Comment:			

No.	Description	Yes	No	N/A
4	Are classified materials stored in an authorized container? (GSA Approved container with supplemental controls for Top Secret; GSA Approved container without supplemental controls for Secret and Confidential; or non-GSA Approved container with supplemental controls for Secret. A non-GSA Approved container is a safe or metal file cabinet having a built-in, three position, combination dial lock with no "GSA Approved" label, or, a metal file cabinet modified with a lock bar and secured with a Sergeant & Greenleaf, three position combination padlock.) Comment:			
5	Have security containers been designated with a number or symbol conspicuously affixed to the outside of the vault or security container? Comment:			
6	Are combinations to security containers and dial-type locks changed by authorized personnel when required? Comment:			
7	Are the combinations to containers used for the storage of classified material properly safeguarded? Comment:			
8	Is Form SF 700, Security Container Information, properly used? Comment:			
9	Are SF 700s properly marked and stored in a separate, authorized container? Comment:			

No.	Description	Yes	No	N/A
10	Is Form SF 702, Security Container Checksheet, properly used? Comment:			
11	Are End-of Day Security Checks conducted? Comment:			
12	Is Form SF 701, Security Activity Checklist, used to record End-of-Day Security Checks? Comment:			
13	Are all security containers used for the storage of classified material physically checked as part of the End-of-Day Security Check? Comment:			
14	Are personnel aware of procedures for conducting classified meetings and conferences? Comment:			
F	**Disposal/Destruction Procedures**			
1	Are classified burn bags properly marked and stored in an appropriate container pending destruction? Comment:			

No.	Description	Yes	No	N/A
2	Is equipment used for the destruction of classified material authorized and approved? Comment:			
3	Are typewriter ribbons, carbons, and other forms of classified waste properly marked and stored, and destroyed by an authorized means? Comment:			
4	Have procedures been established to certify that whenever security equipment is moved or relocated or “out of service” or “excess” that the security equipment does not contain classified information? Comment:			
G	**Reproduction**			
1	Have copiers used for the reproduction of classified been approved for use? Comment:			
2	Are procedures for the reproduction of classified material posted in the immediate vicinity of the copier machine? Comment:			
3	Is classified reproduction avoided or held to an absolute minimum consistent with operational requirements? Comment:			

No.	Description	Yes	No	N/A
H	**Information Systems Security**			
1	Have automated information systems, used for processing classified information, been approved and accredited by the appropriate Designated Accrediting Authority? Comment:			
2	Is the removable hard-drive, laptop, and printer, used for processing classified information properly stored when not in use? Comment:			
3	Are disks and other media containing classified information properly marked and are they properly stored when not in use? Comment:			
4	Has an Information Systems Security Officer (ISSO) been appointed in writing and is the ISSO appropriately cleared? Comment:			
5	Have systems incidents, including the use of unaccredited systems for classified processing, been reported? Comment:			

No.	Description	Yes	No	N/A
6	Has the ISSO been notified of any system changes, including the change of location of equipment? Comment:			

Other Comments: