

ACCOUNTABILITY AND CONTROL OF CLASSIFIED LAPTOP COMPUTERS

I. Purpose

This Instruction implements Department of Homeland Security (DHS) Directive 121-01, and establishes procedures, program responsibilities and reporting protocols for establishing and maintaining accountability and control of laptop computers approved for the processing of classified information.

II. Scope

This Instruction applies to all persons who are permanently or temporarily assigned, attached, or detailed to the Department of Homeland Security (DHS), or other personnel whose duties include the use of classified DHS laptop computers. This Instruction applies to laptops that are owned or leased by DHS and used for processing Classified National Security Information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. This Instruction does not apply to classified laptops owned and used by contractors that are certified, accredited, and under the purview of the Defense Security Service (DSS) in accordance with the National Industrial Security Program (NISP) and its operating manual (NISPOM).

III. Authorities

- A. Title 5, United States Code Annotated App., "The Inspector General Act of 1978," as amended
- B. Title 40, United States Code (U.S.C.), §§ 11101-11703, "Information Technology Management"
- C. Title 44, U.S.C., §§ 3541-3549, "Information Security"
- D. Title 50, U.S.C., Section 401 et seq., "National Security"
- E. DHS Management Directive (MD) 0810.1, "The Office of Inspector General"
- F. DHS MD 4300.1, "Information Technology Systems Security"

- G. DHS 4300B, "National Security Systems Handbook"
- H. DHS MD 11041, "Protection of Classified National Security Information Program Management"
- I. DHS MD 11045, "Protection of Classified National Security Information: Accountability, Control, and Storage"
- J. DHS MD 11049, "Protection of Classified National Security Information: Security Violations and Infractions"
- K. National Security Agency Media Destruction Guidance, <http://www.nsa.gov/ia/government/mdg.cfm?MenuID=10.3.1>

IV. Definitions

- A. **Accreditation (Information System Accreditation)**: The official management decision to permit operation of an Information System in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.
- B. **Certification (Information System Certification)**: The comprehensive evaluation of the technical and non-technical security features of an Information System and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.
- C. **Classification Label**: Standard Form (SF) series labels applied to computer media and hardware to reflect the level of classification the equipment is authorized to process. The labels used shall be the SF 710 for Unclassified; SF 708 for Confidential; SF 707 for Secret; SF 706 for Top Secret; and SF 712 for SCI, or an appropriate label associated with Special Access Program (SAP) information.
- D. **Component Chief Security Officers (CCSO)**: The senior-most Federal security executive designated by the Component head in the following Components:
 - 1. Citizenship and Immigration Services, United States (USCIS)
 - 2. Coast Guard, United States (USCG)
 - 3. Customs and Border Protection, United States (CBP)

4. Federal Emergency Management Agency (FEMA)
5. Federal Law Enforcement Training Center (FLETC)
6. Immigration and Customs Enforcement, United States (ICE)
7. Secret Service, United States (USSS)
8. Transportation Security Administration (TSA)

E. **Designated Accrediting Authority (DAA)**: The DHS official with the authority to assume formal responsibility for operating information systems at an acceptable level of risk. See current version of DHS Handbook 4300B for roles and responsibilities associated with this title.

F. **Government-Furnished Laptop or Notebook Computers**: Laptop or notebook computers that are owned or leased by the U.S. Government.

G. **Information System Security Manager (ISSM)**: The official responsible for the information system security program for a specific Component. See current version of DHS Handbook 4300B for roles and responsibilities associated with this title.

H. **Information System Security Officer (ISSO)**: The person responsible to the ISSM for ensuring that operational security is maintained for a specific information system in accordance with the System Security Authorization Agreement (SSAA). See current version of DHS Handbook 4300B for roles and responsibilities associated with this title.

I. **Key Security Officials (KSO)**: The senior-most Federal security executive designated by the Component head in each of the following Components, or as otherwise identified by the DHS Office of the Chief Security Officer (OCSO):

1. Domestic Nuclear Detection Office (DNDO)
2. Intelligence and Analysis, Office of (I&A)
3. National Protection and Programs Directorate (NPPD)
4. Science and Technology (S&T)

J. **Security Incident**: Any incident that constitutes a security violation or security infraction or alleged/suspected security violation or security infraction.

- K. **Security Infraction**: Any knowing, willful, or negligent action contrary to the requirements of Executive Order 12958, as amended, or its implementing directives, that does not rise to the level of a Security Violation. A Security Infraction is usually a minor incident or administrative error in the safeguarding of classified information that does not result in the compromise of such information or the likelihood of such compromise is remote.
- L. **Security Liaison**: An official who is assigned responsibility for implementing and managing a security program at a Component (where no CCSO or KSO is required) or Subcomponent level as a secondary or additional duty.
- M. **Security Officer**: Authorized Federal position at a Component (where no CCSO or KSO is required) or Subcomponent whose primary duties are to serve as the lead official for developing, implementing, and managing security programs within the applicable Component or Subcomponent.
- N. **Security Official**: A CCSO, KSO, Security Officer or Security Liaison, as applicable.
- O. **Security Violation**: Any knowing, willful, or negligent action: (1) that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) to classify or continue the classification of information contrary to the requirements of Executive Order 12958, as amended, or its implementing directives; or (3) to create or continue a special access program contrary to the requirements of Executive Order 12958, as amended.
- P. **Sensitive Compartmented Information (SCI)**: Classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling within formal access control systems established by the Director of National Intelligence (DNI).
- Q. **Special Access Program (SAP)**: A schedule and supporting procedures established for a specific class of classified information that imposes additional safeguarding and access requirements that exceed those normally required for information at the same classification level.
- R. **System Security Plan (SSP)**: It provides: a complete description of the information system, including purposes and functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, transmissions, and network configuration; an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements; and delineates the responsibilities and expected behavior of all individuals who access the system.

S. **Subcomponent**: An office or administrative entity that falls under the operational and administrative jurisdiction of a DHS Component.

T. **User (Laptop User)**: Any person, to include employees, detailees, and contractors, authorized to access a classified DHS laptop or notebook computer.

V. Responsibilities

A. The **DHS Chief Information Officer (CIO)** is responsible for:

1. Ensuring that policies are in place for the certification and accreditation of laptop computers.
2. Maintaining a master inventory of all laptops within DHS that are certified and accredited for classified processing. This inventory must distinguish classified laptops from all other equipment.
3. Compiling, no less than twice per year, classified laptop inventory reports from Component Chief Information Officers, and accounting for discrepancies of classified laptops not accounted for by disposal, downgrade, or transfer.
4. Providing a copy of each inventory to the DHS Office of the Chief Security Officer, Administrative Security Division (OCSO/ASD).
5. Selecting and facilitating the implementation of an appropriate encryption technology standard for use on classified laptops.

B. The **Component CIOs** are responsible for:

1. Ensuring that policies, consistent with those set by the CIO, are in place for the certification and accreditation of laptop computers within their Component as well as within any other Components they service.
2. Maintaining a master inventory of all laptops within the Component(s) it services that are certified and accredited for classified processing. This inventory must easily distinguish classified laptops from all other equipment.
3. Compiling, no less than twice per year, classified laptop inventory reports from within the Component(s) it services, and accounting for discrepancies of classified laptops not accounted for by disposal, downgrade, or transfer.

4. Providing a copy of each inventory to the Office of the Chief Information Officer (OCIO).

5. Facilitating the implementation of an appropriate encryption technology standard for use on classified laptops.

C. The ***Designated Accrediting Authority (DAA)*** is responsible for ensuring that laptops used for the processing of classified information are appropriately certified and accredited in accordance with the guidance provided in DHS 4300B, National Security Systems Handbook.

D. The ***DHS Chief Security Officer (CSO)*** is responsible for:

1. Administering, managing, and providing oversight for the safeguarding of laptops approved for classified processing.

2. Providing standard security procedures for the storage, transport, and use of classified laptops.

3. Developing procedures for conducting security inquiries or investigations into the loss, theft, misuse, or compromise of classified laptops.

4. Conducting periodic reviews of entities in possession of classified laptops to ensure compliance with safeguarding and classification requirements.

E. The ***Office of the Secretary and Heads of DHS Components*** are responsible for:

1. Ensuring compliance with the security standards for safeguarding classified laptops. The Office of the Secretary and Components without a CIO comply with the requirements of their servicing CIO.

2. Ensuring that an inventory of all classified laptops within the Component is maintained.

3. Ensuring that ISSMs and ISSOs are appointed for classified laptops as required by DHS MD 4300.1.

4. Ensuring that all alleged or suspected incidents of willful employee misconduct, criminal activity, or espionage are reported to the DHS Office of Inspector General (OIG).

- F. The **Information Systems Security Manager (ISSM)** is responsible for:
1. Approving or denying requests for classified laptops from entities within the ISSM's area of responsibility.
 2. Ensuring that all information required to be reported by this Instruction is properly recorded and reported for every classified laptop.
 3. In coordination with the ISSO, ensuring that when a laptop is no longer needed for classified processing, it is properly sanitized or destroyed in accordance with the National Security Information (NSI) Destruction Guidance Manual and the inventory is appropriately updated. Laptops used for SCI and SAP operations will be sanitized under the provisions of Director of Central Intelligence Directive (DCID) 6/3 or successor guidance issued by the Director of National Intelligence (DNI).
 4. Ensuring adequate training is provided to classified laptop users.
 5. Implementing procedures for users to report violations and infractions involving classified laptops to the appropriate Security Official in accordance with DHS MD 11049.
 6. Reporting Security Violations and Infractions involving classified laptops to the appropriate Security Official in accordance with DHS MD 11049 and, as appropriate, DHS Handbook 4300B.
- G. The **Information Systems Security Officer (ISSO)** is responsible for:
1. Ensuring the implementation of security measures, in accordance with the Systems Security Plan (SSP), as an element of the system certification and accreditation package.
 2. Ensuring that changes in laptop classification, location, or responsible user's contact information is properly recorded and reported.
 3. Notifying the ISSM when a laptop is no longer needed for classified processing and ensuring, in coordination with the ISSM, that it is properly sanitized or destroyed in accordance with the National Security Information (NSI) Destruction Guidance Manual and DCID 6/3 or successor guidance issued by the DNI, as appropriate, and inventories are updated.
 4. Coordinating the presentation of classified laptop security training for all users with the servicing Security Official, as appropriate.

5. Ensuring that unauthorized personnel are neither granted use of, nor access to, a classified laptop.
6. Requiring that each user sign an acknowledgement of responsibility for the security of the laptop and classified information prior to accessing the laptop. The attached "User Responsibilities for Issue and Use of a Classified Laptop" is used for this purpose.

H. The **Security Official** is responsible for:

1. Promptly reporting any Security Violation involving a classified laptop to OCSO/ASD and ensuring the conduct of a Preliminary Inquiry/Formal Investigation in accordance with DHS MD 11049. Violations involving SCI and/or SAP information are also reported to the Office of Security, Special Security Programs Division (OCSO/SSPD).
2. Maintaining, in coordination with the ISSM/ISSO, an inventory of all classified laptops in the respective Component to include: classification level, location, and responsible user's contact information.
3. Assisting the ISSM/ISSO in conducting classified laptop inventory activities, as necessary.
4. Conducting or causing to be conducted inquiries or investigations into security incidents involving classified laptops.
5. Ensuring that program reviews and self-inspections conducted in accordance with DHS MD 11041 include the use and storage of classified laptops.
6. Ensuring that all DHS laptops that process Top Secret information are controlled and accounted for as required in DHS MD 11045.
7. Coordinating, together with the ISSM/ISSO, appropriate laptop security training.
8. Maintaining the signed "User Responsibilities for Issue and Use of a Classified Laptop" form for users under their purview.

I. All **Classified Laptop Users** are responsible for:

1. Reading, and then acknowledging, in writing, their responsibilities for the protection of the classified laptop and classified information prior to accessing the laptop. The attached "User Responsibilities for Issue and Use of a Classified Laptop" is used for this purpose and maintained by the servicing ISSO.

2. Reporting any potential or suspected security incident involving classified laptops to the appropriate Security Official in accordance with DHS MD 11049.
3. Complying with all security requirements regarding the use of classified laptops.

VI. Guiding Principles and Procedures

A. Guiding Principles.

1. Prior to the use of a laptop computer for processing classified information, the appropriate DAA must certify and accredit the laptop computers in accordance with the guidance provided in DHS 4300B. Such approval must specify the highest classification level for which the laptop is approved for operation.
2. If a laptop will connect to or function as part of a classified system, the Component CIO or its designee ensures that this is documented in the System Security Plan (SSP) and approved as part of the certification and accreditation process. The SSP is an essential element of the certification and accreditation documentation and defines security controls, characteristics, and guidelines for the system. SAP systems other than SCI are accredited and approved by the OCSO through the OCSO/SSPD.
3. Users will not make modifications to a classified laptop's hardware or software without the approval of the ISSO.
4. Remote access or connection in any form from a classified laptop to any unclassified system is prohibited.
5. Using personally owned laptops for processing classified information is prohibited.
6. Alleged or suspected incidents of willful employee misconduct, criminal activity, or espionage are reported to the DHS OIG.
7. Nothing in this Instruction limits the authority of the OIG as prescribed by DHS MD 0810.1 and the Inspector General Act of 1978, as amended.

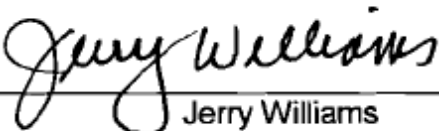
B. **Procedures.**

1. The applicable ISSM must approve in writing requests for the use of a laptop for classified processing, with concurrence from the requestor's supervisor.
2. Classified laptops must be accounted for and discrepancies reported and investigated by the applicable security office and the DHS OIG as appropriate. An inventory of all laptops approved for the processing of classified information is maintained and updated twice per year. The inventory distinguishes those laptops that have been certified and accredited for use in classified processing from all other equipment maintained in the inventory. A copy of each completed inventory is provided to OCSO/ASD.
3. All Security Violations involving classified laptops are reported to the DHS OCSO/ASD in accordance with DHS MD 11049. The servicing Security Official conducts or causes to be conducted a Preliminary Inquiry and/or Formal Investigation in accordance with DHS MD 11049. Security Violations involving SCI or SAP are also reported to OCSO/SSPD.
4. Classified laptops, and unclassified laptops used within a classified environment, must be labeled with the proper SF 700 series label or equivalent. SF 700 Series labels are ordered through the General Services Administration (GSA). Their respective stock numbers are:
 - a. SF 706, Top Secret, Stock No. 7540-01-207-5536
 - b. SF 707, Secret, Stock No. 7540-01-207-5537
 - c. SF 708, Confidential, Stock No. 7540-01-207-5538
 - d. SF 710, Unclassified, Stock No. 7540-01-207-5539
 - e. SF 712, SCI, Stock No. 7540-01-267-1158
5. Classified laptops must be stored in accordance with DHS MD 11045, Section 6.E and transported in accordance with DHS MD 11047, Section VI.
6. All DHS laptops that process Top Secret information are to be controlled and accounted for through a Top Secret Control Officer as referenced in DHS MD 11045, Section 6.B.
7. Laptops that process Sensitive Compartmented Information (SCI) or Special Access Program (SAP) information will be protected and used in accordance with DCIDs 6/3 and 6/9.

8. Classified laptops must employ, as soon as practical, up-to-date encryption technology as stipulated by the DHS CIO. The employment of encryption does not lessen the standards for the safeguarding or storage of a classified laptop or relieve personnel of their responsibility to comply with such safeguarding or storage standards.

VII. Questions

Address questions or concerns regarding this Instruction to the DHS Office of Security.



Jerry Williams
Chief Security Officer

11-3-08
Date

USER RESPONSIBILITIES FOR ISSUE AND USE OF A CLASSIFIED LAPTOP

DEPARTMENT OF HOMELAND SECURITY

USER RESPONSIBILITIES FOR ISSUE AND USE OF A CLASSIFIED LAPTOP

I understand that as a user of a Department of Homeland Security (DHS) laptop that has been approved for processing classified information, it is my responsibility to know and comply with all applicable security measures required for the protection of the equipment and the information it contains.

I have read the Security Plan and Operating Procedures for the equipment to which I shall have access and acknowledge my security responsibilities outlined therein. Additionally, I shall:

1. Comply with the standards and criteria for the classification of information pursuant to Executive Order 12958, as amended, and DHS implementing directives and appropriately mark all classified products in accordance with required classification marking protocols.
2. Administer and maintain all logs, forms, and receipts as required for the applicable level of classification.
3. Protect all media used on the equipment by properly classifying, labeling, controlling, transmitting, and destroying it in accordance with applicable security requirements.
4. Protect all media introduced into the equipment at the highest classification level for which the system is approved, regardless of whether or not classified information was downloaded into the media.
5. Notify the Information Systems Security Officer when access to the system is no longer needed (e.g., transfer, termination, leave of absence, or for any period of extended non-use) or when changes are to occur that affect the security or integrity of the system (e.g., equipment malfunction, change in storage equipment, change in location, etc.).
6. Ensure compliance with software and copyright laws.
7. Report violations or suspected violations involving the improper handling or safeguarding of classified information to the appropriate Security Official.

By signing below I acknowledge and accept the responsibilities associated with my use of a Classified Laptop as stated above and in the Security Plan and Operating Procedures. If I am not a DHS employee, I also acknowledge receipt of a copy of DHS Instruction 121-01-003, *Accountability and Control of Classified Laptop Computers*, and 11049, *Protection of Classified National Security Information: Security Violations and Infractions*.

System User's Signature:		Date:	
Printed Name & Title:			
Division:		Location:	
Phone Number:		Email:	

DHS Form 121-01-003 (10/08)