



Safeguarding Classified & Sensitive Unclassified Information

Reference Pamphlet

Updated March 2007



**Homeland
Security**

Office of Security
Department of Homeland Security
Washington, D.C. 20528

Safeguarding Classified National Security Information and Sensitive but Unclassified Information

Access to classified national security information is a privilege we can not take lightly. Being granted a security clearance means the United States Government has determined us worthy of the trust needed to safeguard national secrets. We therefore have both a legal and a moral obligation to abide by the rules for safeguarding classified information and honor the responsibility with which we have been entrusted.

This pamphlet serves as both an education tool and a quick reference resource for fulfilling your responsibilities on the proper handling and safeguarding of classified information and sensitive but unclassified information. The pamphlet is not all inclusive but does address the basic safeguarding and handling requirements. If additional information or detail is needed, contact your local security official or the DHS Office of Security at the phone number below.

I hope this pamphlet serves you well and helps to quickly answer questions you may have on your safeguarding responsibilities. If you have any comments or suggestions to improve the guide, feel free to contact the Office of Security at (202) 447-5010 or send an email to OfficeofSecurity@dhs.gov. Additional guidance and reference materials can be found at the Security/Administrative Security portal on DHSOnline.

Chief Security Officer/Senior Agency Official
Department of Homeland Security

“The necessity of procuring good intelligence is apparent and need not be further urged. All that remains for me to add is that you keep the whole matter secret as possible. For upon secrecy, success depends in most enterprises of the kind, and for want of it, they are generally defeated.”

George Washington, in a letter to Colonel Elias Dayton, 26 July 1777

Table of Contents

<u>Definitions</u>	Page 4
Classified National Security Information	
Classification Levels	
SCI/SCIF	
Collateral Open Storage	
<u>Classifying Information</u>	Page 4-5
Original Classification Authority (OCA)	
Derivative Classification	
<u>Classification Markings</u>	Page 5-9
Subjects and Titles	
Portion and overall Page Markings	
“Classified By” Line	
“Derived From” Line	
Reasons for Classifying	
Declassification	
Additional Control Notices	
Working Papers	
Computer Tapes, Discs, etc.	
<u>Safeguarding and Storage</u>	Page 10-12
Storage of Classified Information	
Security Container Combinations	
Changing Security Container Combinations	
Use of SF 700, 701 and SF 702	
<u>Access and Control</u>	Page 12-16
Security Clearances	
Need-to-Know/Third Agency Rule	
Cover Sheets (SF 703, 704 & 705)	
Administrative Accountability	
Telephone Use & Other Conversations	
Meetings & Conferences	
Reproduction	
Destruction	
<u>Transmitting/Transporting</u>	Page 16-19
Transmission Requirements	
Packaging	
Receipting	
Local Transport	
<u>Violations/Infractions</u>	Page 18-19
<u>Sensitive but Unclassified Information</u>	Page 19-21
For Official Use Only (FOUO)	
Marking	
Handling Requirements	
Destruction	
Incident Reporting	
<u>Prescribed Forms</u>	Page 22
<u>List of Applicable DHS Management Directives</u>	Page 22

DEFINITIONS

Classified National Security Information: Information that requires protection, pursuant to Executive Order 12958, as amended, against unauthorized disclosure in the interest of National Security.



Classification Levels: All classified information falls within one of three levels: TOP SECRET, SECRET and CONFIDENTIAL. The resulting damage to the national security if the information were released determines the level of classification assigned.

TOP SECRET: Unauthorized disclosure could reasonably be expected to cause *exceptionally grave damage* to the national security.

SECRET: Unauthorized disclosure could reasonably be expected to cause *serious damage* to the national security.

CONFIDENTIAL: Unauthorized disclosure could reasonably be expected to cause *damage* to the national security.

The classification levels cited above are not to be applied to Executive Branch information that is not properly classified national security information.

Sensitive Compartment Information (SCI): Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence or the Director of National Intelligence.

Sensitive Compartmented Information Facility (SCIF): An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed. A SCIF is specifically accredited as a SCIF in accordance with Director of Central Intelligence or Director of National Intelligence issued directives for the primary purpose of storing, using, discussing, and/or processing SCI information. A SCIF should not be confused with other “secure” areas or collateral open storage areas that do not meet SCIF standards and do not fulfill an SCI mission.

Collateral Open Storage Area: A room or area constructed in accordance with DHS Management Directive (MD) Number 11046, “Open Storage Area Standards for Collateral Classified Information,” and authorized in writing by the appropriate DHS official for the open storage of collateral (CONFIDENTIAL, SECRET, TOP SECRET) classified information.

CLASSIFYING INFORMATION

There are two methods in which information is classified – **ORIGINAL** and **DERIVATIVE**.

ORIGINAL CLASSIFICATION is the **INITIAL** determination that information requires, in the interest of national security, protection against unauthorized disclosure. In short, this is information that has not previously had a classification applied. This can only be done by an **Original**

Classification Authority (OCA). OCA's are specifically delegated in writing by position. Refer to DHS Delegation 8100.3, "Delegation of Original Classification Authority," or successor delegations, for the list of positions permanently delegated OCA within DHS. Contact your local security official or the DHS Office of Security for additional delegations.

DERIVATIVE CLASSIFICATION is the act of paraphrasing, restating, or generating in new form, information already classified, and marking the newly developed material consistent with the classification markings existing on the source(s). Derivative classification also occurs through the use of Security Classification Guides. Individuals with the appropriate security clearance, who are required by their work to prepare materials that include existing classified information, can classify derivatively – no additional delegations are necessary.

Persons who derivatively classify or anticipate the need to derivatively classify are encouraged to contact their local security official or the DHS Office of Security/Administrative Security Division (OS/ASD) for assistance and training on the derivative classification process and the marking of classified materials.

CLASSIFICATION MARKINGS

Standard markings must be applied to classified materials. They are applied to **alert the holder** of the classification status of the information and, based on the classification level, prescribe the safeguarding and storage requirements of the information. Therefore, classified materials must be sufficiently marked to eliminate any doubt or uncertainty regarding the classified, or unclassified, status of the information. The following pages provide an explanation and illustration of the standard markings applied to documents or computer media containing classified information.

Subject and Titles

Subjects, titles and similar elements will be parenthetically marked with the level of classification the particular element contains: (TS) = TOP SECRET, (S) = SECRET, (C) = CONFIDENTIAL, and (U) = Unclassified.

Portion Markings

Each paragraph, subparagraph and similar portion will be parenthetically marked with the highest classification of the information contained within the portion, or (U), if it is unclassified.

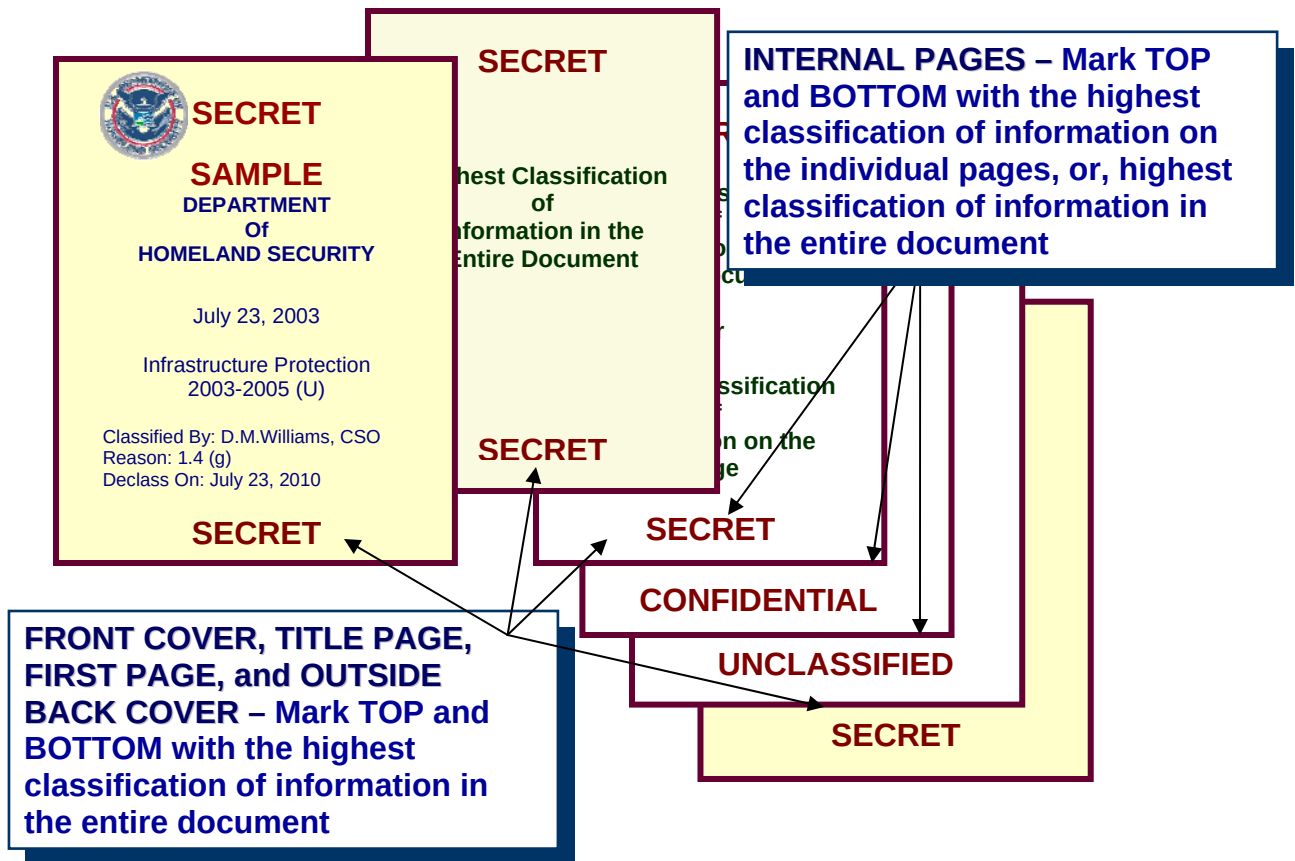
Overall Page Marking

This identifies the highest classification of information contained in the document. The overall classification shall be conspicuously placed at the top and bottom of the front page, title page, first page and back cover, as applicable. Each internal page of a multiple page document will be marked with the highest classification of the information contained on the page, or the highest classification of information contained in the entire document. The latter method may be used to enhance operational efficiency. (See the illustration below.)

The illustration shows a memorandum titled "MEMORANDUM FOR CLASSIFIERS" with the following content:

- SECRET** (at the top and bottom)
- Homeland Security logo
- Date: December 10, 2003
- FROM: Security
- SUBJECT: Subject/Portion Markings (U)
- (C) Note how each subject, paragraph, and subparagraph are individually portion marked.
- (U) The parenthetical marking for each portion reflects the highest classification of information within the portion.
- (S) Portion markings are placed at the end of the subjects and titles and at the beginning of paragraphs, subparagraphs and similar portions.
- Classified by: D.M. Williams, Chief Security Officer
- Reason: 1.4 (g)
- Declassify on: Dec 10, 2008

Arrows from the text blocks on the left point to specific elements in the memorandum: "Subject and Titles" points to the subject line; "Portion Markings" points to the (U) and (S) markings; "Overall Page Marking" points to the SECRET markings at the top and bottom.



CLASSIFICATION ACTIONS

Classification Actions reflect the authority for the information to be classified or the source(s) from where the information was extracted, the reason for classification (for originally classified information only), and how long the information is to remain classified. The classification actions for **originally** and **derivatively** classified material differ slightly and are illustrated on the following pages.

SECRET

July 23, 2003

MEMORANDUM FOR CLASSIFIERS

FROM: Security

SUBJECT: Classification Actions (U)

(C) Classification actions for an originally classified document will include:

(S) The "Classified By" line will identify the delegated original classification authority by name and position.

(U) The "Reason" line will cite the specific reason for classification per Section 1.4 of EO 12958, as amended.

(U) The "Declassify On" line will cite one of the following: a specific date or event within ten years, a date ten years from date of origination, or a date up to 25 years from date of origination.

Classified By: D.M.Williams, CSO
Reason: 1.4(g)
Declass On: Dec 10, 2008

SECRET

Originally Classified Document:

The classification actions for an originally classified document are:

"Classified By" Line: Identifies the approved and delegated Original Classification Authority by name and position.

"Reason" Line: Identifies the specific reason for classification per Section 1.4 of E.O. 12958, as amended.

"Declassify On" Line: Identifies the specific date or event within 10 years when the information is to be declassified, or, a date 10 years from the date of origination, or, a date within 25 years from the date of origination, as determined by the original classification authority.

Derivatively Classified Documents:

The classification actions for a derivatively classified document are:

“Derived From” Line: Identifies the source of the information, including the agency/office of origin and date of the source document. If two or more classified sources are used then the “Derived From” line will read “Multiple Sources.” A record of the classified sources used will be maintained with the file or record copy of the document.

“Declassify On” Line: Identifies the declassification instruction as stated on the source. Where multiple sources are used, the most restrictive declassification instruction will be applied.

Revisions to Executive Order 12958, as amended (March 2003), and 32 CFR, Part 2001/2004, Information Security Oversight Office (ISOO), Directive No. 1, Classified National Security Information, (September 2003), resulted in the elimination of exemptions to the 10 Year Rule as a declassification instruction (i.e., X-1 thru X-8). The use of X-1 thru X-8 as a stand-alone declassification instruction on original or derivatively classified documents created after September 22, 2003, is **PROHIBITED**. When deriving classified information from a source document that is dated before September 22, 2003, and the source document cites an X-1 thru X-8 exemption as a declassification instruction, the declassification instruction of the newly created document will be marked: “Source Marked X-(enter appropriate exemption number(s) as cited on the source), Date of Source: (enter the date of the classified source document from which the classified information was derived). Where multiple sources were used enter the date of the most recent source. (NOTE: The date of the source shall not exceed September 21, 2003.) For Example:

Declass On: Source Marked X-1, Date of Source September 21, 2003

If a source document has a date of September 22, 2003, or later, and the declassification instruction on that source document is an X-1 thru X-8 exemption, the newly created document will cite a declassification instruction of September 22, 2028.

Similarly, if a source document has a declassification instruction of “OADR” (which under predecessor Executive Orders meant “Originating Agency Determination Required”), the same shall apply except the date of the source shall not exceed October 13, 1995. For Example:

Declass On: Source Marked OADR, Date of Source Oct 13, 1995

SECRET  July 23, 2003 MEMORANDUM FOR CLASSIFIERS FROM: Security SUBJECT: Classification Actions (U) (U) Classification actions for a derivatively classified document will include: (S) The “Derived From” line citing the specific source from where the classified information came from. At a minimum, this will include the agency/office name, subject/title of the source, and the date of the source. (U) A “Reason” line is not required on derivatively classified documents. (U) The “Declassify On” line will carry forward the same declassification instruction as cited on the source. Where multiple sources are used – carry forward the most restrictive declassification instruction. → Derived From: DHS OS Memo, Subj: Training (U) Dtd Jul 1, 2003 → Declass On: Dec 31, 2010 SECRET
--

Additional Control Notices: Additional Control Notices are “caveats” prescribed by Director Central Intelligence Directive (DCID) 6/6, “Security Controls on the Dissemination of Intelligence Information,” or successor Director of National Intelligence (DNI) directives, as a means to further restrict or control access to certain types of information. Examples of these caveats are:

- NOFORN – “Not Releasable to Foreign Nations”
- PROPIN – “Caution – Proprietary Information Involved”
- ORCON – “Dissemination and Extraction of Information Controlled By Originator”

When caveated information is carried forward into a newly created document (derivative classification), the caveat will also be applied to the newly created document and complied with.

Marking Sensitive Compartmented Information (SCI) and Special Access Program Materials (SAP): Materials containing SCI and/or SAP information will be marked in accordance with DCI or DNI directives and applicable program guidance. Contact your Special Security Officer (SSO) for guidance.

Classified Working Papers: Classified Working Papers are documents or materials, regardless of the media, that are expected to be revised before preparation of a finished product. For the most part, they are considered “Drafts” and not intended for dissemination or retention. Working papers containing classified materials will:

- be dated when created;
- identify the creator of the document; _____
- marked with the highest classification of information they contain; _____
- protected commensurate with the classification level;
- be destroyed in an approved manner when no longer needed.

Classified working papers will be marked and controlled in the same manner as a finished document of the same classification if:

- they are released by the originator outside of the originating activity;
- they are retained for more than 180 days from the date created, or;
- they are filed permanently.

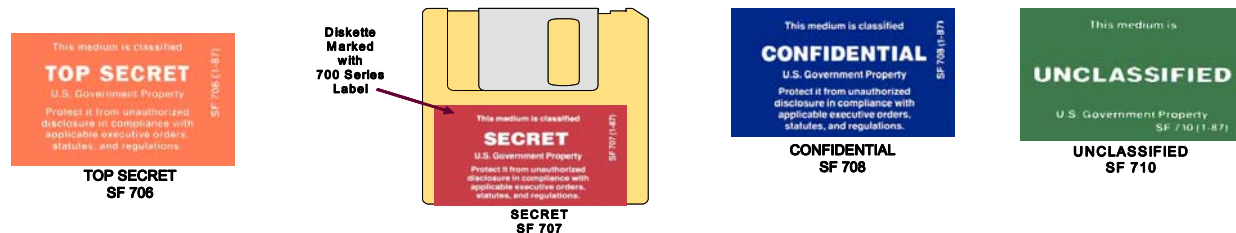
Marking in the same manner as a finished document refers to the application of appropriate markings, i.e., portion markings, classification actions and any other markings as cited on the previous pages.

SECRET	12/2/03
Notes from meeting with CBP and DOJ Criminal Division	
We discussed the case of S Claus and determined border crossings for the purpose of distributing unregulated contraband was a violation of US sovereignty.	
A plan will be developed and documents issued to circumvent the illegality so S Claus can continue the annual mission without breaking the law. DOD coordination will be required.	
We will meet again, along with DOD reps, on Dec 24, 2003.	
K.D. Winslow, DHS Security	
SECRET	

SECRET	12/2/03
(U)	Notes from meeting with Customs and DOJ Criminal Division
(S)	We discussed the case of S Claus and determined border crossings for the purpose of distributing unregulated contraband was a violation of US sovereignty.
(C)	A plan will be developed and documents issued to circumvent the illegality so S Claus can continue the annual mission without breaking the law. DOD coordination will be required.
(U)	We will meet again, along with DOD reps, on Dec 24, 2003.
K.D. Winslow, DHS Security	
Derived From DOJ SCG Dtd. 12/12/2002	
Declass On: 12/31/2010	
SECRET	

Marking Classified Diskettes and Other Media:

Diskettes, computers, laptops, and other media used for processing classified information will be marked with the highest classification of information ever stored or the highest classification level of media that it has come into contact with. Standard Form (SF) 700 series labels will be used for this purpose.



When not in use, classified diskettes will be stored in approved security containers. The equipment processing the information, i.e., removable hard drive, Laptops, PC, etc, will also be identified through the use of SF 700 series labels. The SF 700 series labels used will be based on the Classification level the system has been accredited for.

NOTE: Classified information must not be processed on any automated equipment unless the equipment has been specifically accredited and approved for classified processing by an authorized official. Contact your local Information Systems Security Manager or Security Official for guidance.

SAFEGUARDING & STORAGE

Classified information created by or entrusted to DHS will be protected from unauthorized disclosure. The following are the standards for the storage of classified materials. Refer to DHS Management Directive (MD) 11045, "Protection of Classified National Security Information, Accountability, Control and Storage," for additional information.

TOP SECRET must be stored in:

A safe type steel file container having a built in, three position, dial-type, combination lock approved by GSA and bearing the GSA approval label. One or more of the following supplemental controls will also be in place:

- The location housing the security container is subject to continuous protection by cleared guard or duty personnel,
- Cleared guard or duty personnel inspect the container every two hours, or,
- The location is protected by an Intrusion Detection System with a personnel response time within 15 minutes of initial alarm annunciation.



SECRET must be stored in:

A GSA Approved container bearing the GSA Approved label.
When stored in a GSA Approved container, supplemental controls are not required.

Or,

A non-GSA Approved safe type steel file container having a built-in three position combination lock but no GSA Approved label, or a lock-bar cabinet equipped with a steel bar held in place across the drawer fronts and secured with a Sergeant & Greenleaf three position combination padlock (modification in this manner of existing filing cabinets for classified storage is not authorized). When stored in this manner, one or more of the following supplemental controls listed above is required with the following modifications:



- Guard or duty personnel checks conducted every four hours and;
- Alarm response is 30 minutes.

CONFIDENTIAL must be stored in:

A manner prescribed for the storage of TOP SECRET or SECRET material. When CONFIDENTIAL materials are stored in a non-GSA Approved container, supplemental controls are not required.

TOP SECRET, SECRET, or CONFIDENTIAL materials can also be stored in a certified and approved vault or Open Storage Area. Refer to DHS MD 11046 or contact the DHS Office of Security, Administrative Security Division or your local security official for guidance.

NOTE: Effective October 1, 2012, the use of non-GSA Approved containers for the storage of SECRET or CONFIDENTIAL classified materials will not be authorized.

Security Container Combinations

Combinations to dial-type locks are classified at the level of the highest classification of the information stored in the container. Combinations are to be changed by persons having an appropriate security clearance and who have received instructions on how to change them. Contact a security official for assistance. Container combinations will be changed:

- When containers are first placed into or taken out of service
- When a person with knowledge of the combination no longer requires access to it
- When the possibility of a compromise exists
- At least every two years

SF 700, Security Container Information

The SF 700 comes in 3 parts and is used to record the container combination and the personnel who should be contacted in the event of an emergency.

Part 1-Completed and posted on the inside of the locking drawer of the container.

Part 2-Is a carbon copy of **Part 1**, and also serves as an envelope for **Part 2A**.

Part 2A-Is used to record the combination of the container, When **Part 2A** is completed it is inserted into **Part 2**. **Part 2** is then sealed and marked with the highest classification of materials in the container. **Part 2** is then stored in a secure, central location, normally by your local security official.

This image shows the top portion of the SF 700 form. It is divided into two main sections. The left section, labeled 'Part 1 & 2', contains fields for '1. COMPLETE PART 1 AND ATTACH TO INSIDE OF CONTAINER' and '2. DETACH PART 2 AND INSERT IN ENVELOPE'. The right section, labeled 'Part 2A', contains fields for '3. ROOM NO.', '4. DATE COMBINATION', and '5. DATE COMBINATION CHANGED'. The form is titled 'SECURITY CONTAINER INFORMATION' and 'STANDARD FORM 700 (8-81)'.

Part 1 is filled out, detached from **Part 2**, and posted on the inside of the container.

Part 2A is completed and inserted into **Part 2**.

Part 2 is marked with the appropriate classification marking and stored in a secure, central location.

This image shows the bottom portion of the SF 700 form. It is divided into two main sections. The left section, labeled 'Part 2', contains fields for '6. ROOM NO.', '7. DATE COMBINATION', and '8. DATE COMBINATION CHANGED'. The right section, labeled 'Part 2A', contains fields for '9. ROOM NO.', '10. DATE COMBINATION', and '11. DATE COMBINATION CHANGED'. The form is titled 'SECURITY CONTAINER INFORMATION' and 'STANDARD FORM 700 (8-81)'. The word 'SECRET' is printed in large red letters across the top and bottom of the form.

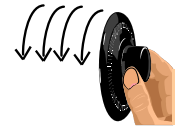
SF 702, Container Check Sheet

The SF 702 is used to record the dates, times, and initials of when and who opened, closed, or checked a particular security container or vault. The form is attached to the outside or in the immediate vicinity of the security container or vault.

SF 701, Activity Security Checklist (End-of-Day Security Checks)

Any room or area in which classified information is stored, handled, or processed will develop and implement an End-of-Day Security Check Program. The purpose of the check is to ensure classified materials are secured before the area is vacated at the end of the day. The SF 701, "Activity Security Checklist," is used for recording the end of day check. The SF 701 can be maintained anywhere within the applicable area but is often posted in the immediate vicinity of the area exit for convenience and to serve as a reminder to the checker. Checks should be conducted by a cleared person as close to the end of the work day as possible. The following should be included as part of the End-of-Day security check:

- ✓ Check all containers used for the storage of classified material. Spin the combination dial at least four times and physically pull each drawer to ensure all drawers are secure.



- ✓ Check secure telephones to ensure the keys or cards to each unit are not inserted or are not in the immediate vicinity of the unit.
- ✓ Visually inspect desktops and wastebaskets for the presence of classified materials.
- ✓ Ensure computers are logged off.
- ✓ Visually inspect copiers, fax machines, and printers to ensure there are no classified materials in, on, or near the devices.
- ✓ Check other items and devices as deemed necessary for your particular work area.

ACCESS & CONTROL

Before access to classified information is granted, three criteria will be met:

- The intended recipient possesses a security clearance equal to or greater than the classification of the information disclosed.

The security clearance of DHS personnel can be verified by contacting the DHS Office of Security Customer Service Center at (202) 447-5010.

- The intended recipient has a Need-to-Know.

Need-to-Know is the determination that an individual who possesses a security clearance requires access to classified information in the performance of his/her official duties. No person is entitled access to classified information solely by virtue of office, position, rank or security clearance. Determination of need-to-know is the responsibility of the holder of the classified information.

- The intended recipient has the capability to properly safeguard and store the materials.

Prior to transferring or transmitting classified materials, the holder of the materials must ensure the intended recipient has the means to store the materials in accordance with DHS requirements. This is done by simply asking the person.

Personnel shall comply with any access and/or dissemination restrictions cited on the document. Information originated by another government agency shall not be further disseminated to a third party without prior approval of the originator.

COVER SHEETS (SF 703,704 & 705)

When removed from storage, classified materials will be kept under constant surveillance, and, when not in immediate use, covered with a standard coversheet. Cover sheets to be used are:

SF 703-TOP SECRET



SF 704-SECRET



SF 705-CONFIDENTIAL



Administrative Accountability

All classified information is accountable. However, only certain types of classified information require the maintenance of administrative accountability records. The Level of classification will determine the degree of administrative accountability.

- **TOP SECRET:** Program offices that routinely store or handle TOP SECRET information will establish a TOP SECRET Control Account (TSCA) and appoint a TOP SECRET Control Officer (TSCO) and as many alternates as are necessary to efficiently manage the account. The TSCO will be responsible for maintaining accountability records for the control and disposition of all TOP SECRET information maintained in the TSCA. Additionally, an inventory of documents in a TSCA will be conducted before December 31, of each year. There is no need to establish a TSCA and appoint a TSCO if a program office does not handle TOP SECRET information. Refer to DHS Management Directive 11045, "Protection of Classified National Security Information, Accountability, Control, and Storage," for additional information.
- **SECRET and CONFIDENTIAL:** Accountability records for SECRET or CONFIDENTIAL information are not required unless specifically directed by the originator of the information or governed by program guidance, e.g., NATO.

Telephone Use and Other Classified Conversations

Never discuss or try to talk around classified information over an unsecured telephone system. Classified telephone discussions must be conducted using secure equipment, e.g., Secure Telephone Unit (STU-III) or Secure Telephone Equipment (STE).



Before holding a classified discussion on an approved phone ensure the person on the distant end possesses the appropriate security clearance and the need-to-know for the information being discussed. The discussion cannot exceed the level of classification for which the STU/STE connection is approved.

You must also ensure the classified portion of the conversation is not overheard by uncleared personnel. Most offices are not soundproof and voices tend to carry into adjacent cubicles and hallways. Always check adjacent areas to prevent unauthorized persons from overhearing classified discussions.

Never discuss classified or sensitive information in an unsecure area. Such information shall never be discussed in public areas, planes, trains, shuttle buses, restaurants, taxis, or in any other circumstance where the possibility exists that unauthorized persons may overhear the conversation.

Classified Meetings and Conferences

Special care must be taken when coordinating the conduct of meetings, conferences, seminars, and other symposia in which classified information will be present. Contact your security official or refer to DHS MD 11045, "Accountability, Control, and Storage," for more information.

For in-house gatherings and other impromptu meetings in which 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:

NOTE: Under no circumstances will SCI be discussed in an area that has not been specifically approved and accredited for SCI discussion.

- The meeting is held in an area under security control of a US Government agency or at an appropriately cleared US contractor facility.
- Ensure all electronic equipment maintained in the room that is capable of transmitting signals outside the room is powered off.
- Conduct a sound attenuation test to ensure normal conversation from inside the room cannot be heard intelligibly 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.
- Assign and post cleared host office personnel at exterior doors and hallways to keep the room's perimeter under surveillance and prevent individuals from stopping and listening.
- Control access to the room, use an attendee roster if applicable, and have sufficient backup host office personnel available as needed.
- Verify the identity of each participant via U.S. Government photo-identification or similar documentation.
- Ensure the security clearances of attendees are at least equal to the level of classified information to be disclosed.
- Prohibit those without proper authorization and clearance from attending classified portion(s).
- Notify each attendee and presenter(s) of:
 - The highest level of classified information to be presented/discussed and when multiple presentations are given, the specific classification (or unclassified status) of each.

- The entrance and the access controls prior to/during the meeting to prevent access by unauthorized personnel.
 - 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.
- Ensure security protection of the room is maintained during breaks.
 - Comply with all security safeguards for classified information.
 - At the conclusion of the meeting conduct an inspection of the room to ensure no classified materials have been left behind.
 - If applicable, ensure sufficient supplies are available to properly package and transport classified information for local attendees to hand-carry classified information back to their offices. For anyone outside the local area, gather, package and mail classified materials to the attendee's office.

Reproduction of Classified materials

The following guidelines govern the reproduction of classified material:

- Reproduction of classified will be kept to an absolute minimum, consistent with operational requirements.
- Honor any reproduction restrictions cited.
- If there is uncertainty over the authority to reproduce, contact the originator for approval.
- Coordinate reproduction of TOP SECRET materials with the applicable TOP SECRET Control Officer.
- Reproduction must not be done on machines connected to an unclassified LAN, remote diagnostics or on machines equipped with a hard-drive or that otherwise retain memory or images.
- Reproduced copies of classified materials are subject to the same safeguards, controls, and accountability procedures as the original.

Destruction of Classified Materials

Classified materials will be destroyed in an approved manner. Most collateral classified paper products can be destroyed using existing cross-cut shredders with a particle size of the cuts not exceeding 1/32 X 1/2 inch. New shredders purchased for use in destroying classified materials will comply with the standards cited in Committee on National Security Systems (CNSS) Policy No. 16 and included on the National Security Agency (NSA) Evaluated Products List. For additional information on shredders contact your local security official or the DHS Office of Security, Administrative Security Division, or visit the Security/Administrative Security portal on DHSOnline.

COMSEC paper products will be destroyed in accordance with CNSS Policy No. 16.

Classified computer media will be destroyed in accordance with guidance published by the Office of the Chief Information Officer.

Two cleared personnel must be involved in the destruction of TOP SECRET materials – one to destroy and one to witness the destruction. Both individuals must have a clearance at or above the material being destroyed. A Certificate of Destruction will be used to record the destruction.

Only one cleared person is needed to destroy SECRET and CONFIDENTIAL. A destruction certificate is not required.

TRANSMITTING & TRANSPORTING CLASSIFIED MATERIAL

Transmission Requirements

Transmission of **TOP SECRET** information within the U.S. or between the U.S. and Puerto Rico or a U.S. possession or Trust Territory can be accomplished as follows:

- Direct person-to-person contact between cleared persons. Contact your security official or refer to DHS MD 11047, “Transmission & Transportation,” for information on courier designations.
- Defense Courier Service (DCS) or other authorized government agency courier service.
- Electronic means over NSA approved communications system(s).
- STU III/STE/Secure fax keyed to the appropriate level.

NOTE: Never enter TOP SECRET materials into any mailing system.

Transmission of **SECRET** and **CONFIDENTIAL** material within the U.S. and between the U.S., Puerto Rico or a U.S. possession or Trust Territory can be accomplished as follows:

- Any means approved for **TOP SECRET**.
- U.S. Postal Service Registered Mail.
- U.S. Postal Service Express Mail. The “Waiver of Signature and Indemnity” block, Item 11b of the mailing label, must NOT be completed and street-side collection boxes will not be used.
- Federal Express; UPS; Airborne Express; AirNet Systems; Associated Global Systems; Cavalier Logistics Management; CorTrans Logistics; DHL Airways; or Menlo Worldwide Forwarding (formerly Emery). These carriers shall **ONLY** be used as a last resort and **ONLY** on an exceptional basis when an urgent requirement exists for overnight delivery. Contact your Security Official or refer to DHS Management Directive 11047, “Protection of Classified National Security Information, Transmission & Transportation,” for additional restrictions and information.
- Cleared commercial or messenger service.

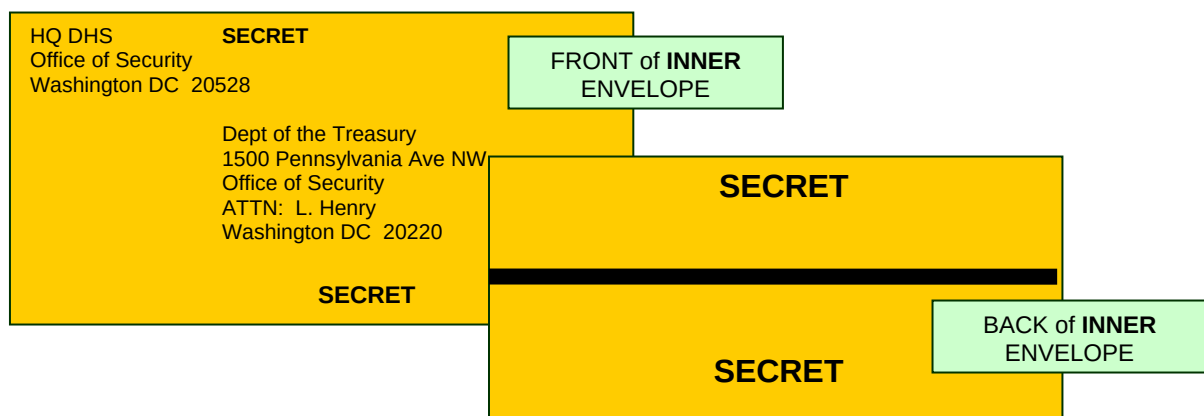
Transmission of classified materials overseas can be accomplished as follows:

- U.S. Postal Service Registered Mail (SECRET and CONFIDENTIAL ONLY) if sent through a military postal service facility, i.e., APO/FPO.
- Department of State Courier System (Diplomatic Pouch).
- Electronically, over an NSA approved communication system.

Packaging of Classified materials

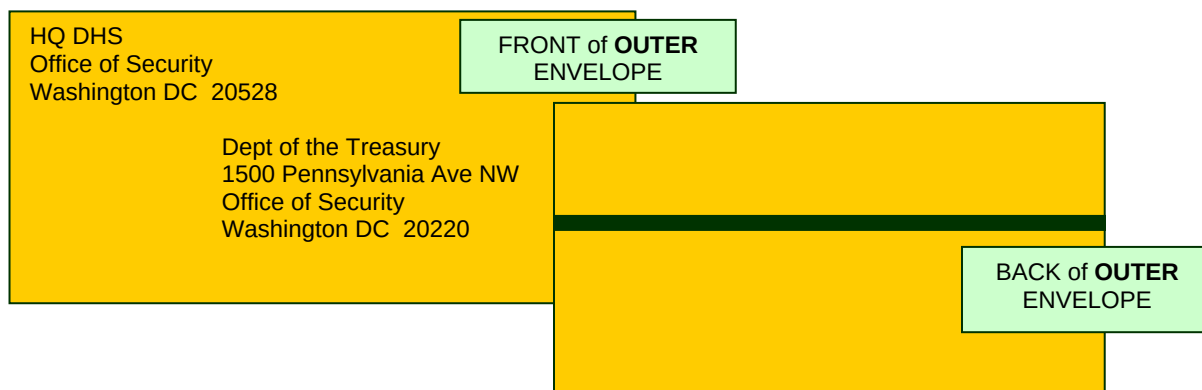
Classified materials must be properly packaged prior to shipment or transfer.

- Cover materials with an appropriate coversheet.
- Place the materials in an opaque envelope, hereafter referred to as the “**inner**” envelope.
Mark the **inner** envelope with the complete name and address of the sender and recipient, to include an “Attention” line. Personal names will be used on the **inner** envelope only.
Conspicuously mark the front and back of the **inner** envelope with the highest classification of the material it contains.
- Seal the envelope with nylon reinforced or similar reinforced tape.
- Complete and attach a document receipt to the **inner** envelope, listing all classified materials transmitted.



Place the **inner** envelope inside a second opaque envelope, hereafter referred to as the “**outer**” envelope.

- Mark the **outer** envelope with the complete address, to include the program office, of the sender and recipient.
- **DO NOT** mark the outer envelope with the classification level of the information it contains, or in any manner to reveal the envelope contains classified material.
- **DO NOT** include personal names on the **outer** envelope.



Notice there are no classification markings on either the front or back of the **outer** envelope. There should be no markings on the **outer** envelope to indicate it contains classified materials.

Receipts

Classified materials transmitted outside of a program office should be accompanied by a document receipt. Receipts are required for the transfer of SECRET and TOP SECRET materials and optional for the transfer of CONFIDENTIAL materials. DHS Form 11000-11, "Document Record of Transmittal," may be used for this purpose.

Hand-carrying Classified in the Local Area

When classified materials are hand-carried outside of a building within the local area, they will be wrapped in the manner prescribed in the previous pages. If a locked briefcase or similar locked case is used the locked case can serve as the "outer" packaging.

When classified materials are hand-carried outside the office but within the confines of a building, they need not be wrapped as prescribed previously, but they must be inserted in an unmarked file folder or envelope in order to avoid unnecessary attention.

Persons who will hand-carry classified materials outside of a building shall first be designated as classified couriers and provided with briefings on their responsibilities while in transit. Contact your security official or refer to DHS MD 11047 for information on classified courier designations and obtaining written courier authorization.

VIOLATIONS/INFRACTIONS

The responsibility for maintaining the security of classified information rests with each person having knowledge or physical custody of that material. Any employee or contractor who observes a security violation or infraction must immediately report it to their supervisor or a security official.

Upon receipt of a report, an inquiry will be conducted to determine the nature of the incident and if a compromise of classified information occurred. Another purpose of the inquiry is to expose and analyze any weaknesses and/or vulnerabilities in the programs in place for the protection of classified information and develop procedures to prevent similar instances from recurring.

If the violation or infraction involves unsecured or unattended classified material, secure the materials in an appropriate manner until they can be brought back under proper security controls. The following are some examples of violations/infractions that should be reported.

- Leaving a classified file or security container unlocked and unattended
- Keeping classified material in a desk or unauthorized cabinet
- Leaving classified material unsecured or unattended on a desk, tables, cabinets, or elsewhere in an unsecure area



- Reproducing or transmitting classified material in an unsecure manner and/or without proper authority
- Taking classified material home without first obtaining specific approval and having the appropriate security equipment in place
- Granting a person access to classified information without first verifying security clearance and need-to-know
- Discussing classified information over an unsecure telephone
- Discussing classified information in public areas
- Failing to secure and store combinations to safes used for the storage of classified materials in an appropriate manner, e.g., writing them down on note pads, keeping them in a desk drawer or rolodex, carrying them in a wallet, etc.
- Failure to properly mark classified materials
- Failure to properly destroy classified materials

This list is not all inclusive. Report to your security officer ANY situation in which you feel that an incident has occurred.

SENSITIVE BUT UNCLASSIFIED INFORMATION

For Official Use Only (FOUO)

FOUO is the designator used within DHS to identify Sensitive but Unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. For example, information designated as Protected Critical Infrastructure Information (PCII) and Sensitive Security Information (SSI) is governed by separate guidance issued by the responsible program office.

For additional guidance on FOUO refer to DHS Management Directive (MD) 11042.1, "Sensitive but Unclassified (For Official Use Only) Information." For guidance on SSI refer to DHS MD 11056, "Sensitive Security Information," or, 49 CFR Part 1520. For guidance on PCII refer to 6 CFR Part 29.

Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," "Official Use Only (OUO)" and "Law Enforcement Sensitive (LES)." In most instances the safeguarding requirements for these types of information are equivalent to FOUO. However, these other agencies may have additional requirements concerning the safeguarding of sensitive information. When available, follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for FOUO as provided in DHS MD 11042.1.

Any DHS Employee, Detailee, or Contractor can designate information as FOUO provided it meets the sensitivity threshold represented by the FOUO definition cited above and it falls within one of the categories of information listed in MD 11042.1 as FOUO. Officials occupying supervisory or

managerial positions are authorized to designate other information, not listed in the MD and originating under their jurisdiction, as FOUO.

The FOUO designation shall NOT be applied to any information in order to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency.

Marking

Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. At a minimum, prominently mark on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO information may be further marked with an applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Additional access and dissemination restrictions may also be cited as the situation warrants.

Designator or originator information & markings, downgrading instructions, & date/event markings are not required on FOUO documents.

Access and Dissemination

A security clearance is not required for access to FOUO information.

Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator.

FOUO information may be shared with other agencies, Federal, state, tribal, or local government and law enforcement officials, provided a need-to-know has been established and the information is shared in the furtherance of a coordinated and official governmental activity, to include homeland defense.

When discussing FOUO information over a telephone, the Secure Telephone Unite (STU-III) or Secure Telephone Equipment (STE) is encouraged, but not required.

FOUO information may be transmitted via non-secure fax machine, although the use of a secure fax is encouraged. Where a non-secure fax machine is used ensure that the materials faxed will not be left unattended or subject to unauthorized disclosure on the receiving end.

FOUO information may be transmitted over regular email channels. However, it shall not be sent to personal email accounts. For added security when transmitting FOUO information by email, password protected attachments may be used with the password transmitted or otherwise communicated separately.

FOUO information shall not be entered or posted on any public website.

FOUO information may be mailed by regular US Postal Service first class mail or any commercial mailing service.

Storage

When unattended, FOUO information will be stored in a locked filing cabinet, locked desk drawer, a locked overhead storage compartment such as systems furniture credenza, or a similar locked compartment. Information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without the need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

Destruction

- Hard copy FOUO materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition and reconstruction.
- After destruction, materials may be disposed of with normal waste.
- Electronic storage media shall be sanitized appropriately by overwriting or degaussing.
- **Paper products or electronic media containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have been destroyed as specified above.**

Incident Reporting

- Incidents involving FOUO material on DHS information systems will be reported to the organizational element's computer security incident response center (CSIRC).
- Suspicious or inappropriate requests for information shall be immediately reported to the DHS Office of Security.
- At the request of the originator, an inquiry will be conducted by the local Security Official or other designee to determine the cause and effect of the incident, and the appropriateness of administrative and disciplinary action against the offender.

Prescribed Forms:

Forms Obtained Thru GSA:

Form No.	Stock No.
SF 700, Security Container Info	7540-01-214-5372
SF 701, Activity Security Check Sheet	7540-01-213-7899
SF 702, Sec Container Check Sheet	7540-01-213-7900
SF 703, TOP SECRET Cover Sheet	7540-01-213-7901
SF 704, SECRET Cover Sheet	7540-01-213-7902
SF 705, CONFIDENTIAL Cover Sheet	7540-01-213-7903
TOP SECRET Rubber Stamp	7520-01-207-4118
SECRET Rubber Stamp	7520-01-207-4119
CONFIDENTIAL Rubber Stamp	7520-01-419-5949
Unclassified Rubber Stamp	7520-01-207-4242
Computer Media Labels (Stickers)	
SF 706, TOP SECRET	7540-01-207-5536
SF 707, SECRET	7540-01-207-5537
SF 708, CONFIDENTIAL	7540-01-207-5538
SF 710, Unclassified	7540-01-207-5539

DHS Management Directives (MD) for Classified and FOUO Information:

- **DHS MD 11004, Security Compliance Review Program
- **DHS MD 11022, Accountability and Control of Classified Laptops
- DHS MD 11035, Industrial Security Program
- **DHS MD 11038, Classified North Atlantic Treaty Organization (NATO) Information
- DHS MD 11041, Protection of Classified National Security Information, Program Management
- DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS MD 11044, Protection of Classified National Security Information, Classification Management
- DHS MD 11045, Protection of Classified National Security Information, Accountability, Control and Storage
- DHS MD 11046, Open Storage Area Standards for Collateral Classified Information
- DHS MD 11047, Protection of Classified National Security Information, Transmission and Transportation
- DHS MD 11049, Security Violations and Infractions
- DHS MD 11056, Sensitive Security Information
- **DHS MD 11057, Identifying and Protecting Restricted Data and Formerly Restricted Data

** Directive is currently under review/pending publication. When approved and published, as with the other directives already published, it will be posted on the Security/Administrative Security portal on DHSONline.

Other Important DHS Publications Dealing with Classification:

- 6 CFR Part 7, DHS Implementation of the Classified National Security Information Program
- DHS Delegation 8100.3, Delegation of Original Classification Authorities
- DHS Delegation 12001, Delegation of Emergency Authority to Disseminate Classified Information
- Secretary DHS Memorandum, March 3, 2004, Designation of Senior Agency Official

**Questions or concerns relative to any security issue may be addressed to the
DHS Office of Security Customer Service Center:
(202) 447-5010**