Safeguarding Classified and Sensitive But Unclassified Information

Reference Booklet for State, Local, Tribal and Private Sector Programs

Updated May 2005

Homeland Security

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

FORWARD

The Department of Homeland Security has been tasked by the President to take a lead role in establishing lines of communication for information sharing between the Federal, State, Local, Tribal, and Private Sector agencies and personnel. This information sharing is necessary to ensure that appropriate officials at all government levels and within the law enforcement and private sector communities have as much relevant real-time information practical to protect and defend against threats to the homeland.

Because of the sensitive nature of certain types of information, it is essential that access and dissemination be controlled and restricted in order to prevent compromise. The unauthorized release or inadvertent disclosure of such information could, among other things, adversely affect our ability to detect an adversary's intentions, neutralize our offensive capabilities in the pursuit of terrorists, compromise the identity of a confidential human source or operation, or result in physical harm to our citizens. While it is in the nation's best interest to form and sustain an active and robust exchange of information for the defense of the homeland, we must still be ever mindful of the damage to our national security that could occur should such information be released to persons who do not have an appropriate security clearance or need-to-know.

This booklet was created to provide you with a quick reference on the rules for safeguarding classified information and 'sensitive but unclassified' information and to help you fulfill the responsibilities inherent upon the granting of a security clearance and accessing sensitive information. I hope it serves you well, but don't consider it as your only source for guidance on the classification process. If you have questions or need additional assistance, please don't hesitate to call us - we'll be happy to help.

Chief Security Officer/Senior Agency Official
Department of Homeland Security

> "The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information."
>
> **Homeland Security Act of 2002, Section 891**

REFERENCES

- Executive Order 12958, as amended, "Classified National Security Information"
    - The full text of Executive Order 12958, as amended, is available at National Archives and Records Administration (NARA) website at: http://www.archives.gov/about_us/basic_laws_and_authorities/appendix_12958.html
- Information Security Oversight Office (ISOO) Directive No. 1 (32 CFR, Part 2001), "Implementing Directive for Executive Order 12958, as amended"
    - The full text of 32 CFR, Part 2001 is available at NARA's website at: http://www.archives.gov/isoo/rules_and_regulations/eo_12958_implementing_directive.html
- Executive Order 12968, "Access to Classified Information"
    - The full text of Executive Order 12968, is available at the Defense Security Service website at: http://www.dss.mil/seclib/eo12968.htm

DHS Management Directives (MD) for Classified and "For Official Use Only" Information

- DHS MD 11035, Industrial Security Program
- 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 11050.2, Personnel Security and Suitability Program
- **DHS MD 11047, Protection of Classified National Security Information, Transmission and Transportation

** - Directive is currently under review/pending publication.

CONTACT INFORMATION

Questions or comments relating to this handbook can be addressed to:

Department of Homeland Security
Office of Security/Administrative Security Division (DHS OS/ASD)
Washington D.C. 20528

Telephone: (202) 401-6173
Fax: (202) 772-9915
E-mail: charlie.rogers@dhs.gov
AdminSecurity@hq.dhs.gov

"Damage to National Security – harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as sensitivity, value, utility, and provenance of that information.."

Executive Order 12958, as amended, Section 6.1

TABLE of CONTENTS

SECTION I:
Safeguarding Classified National Security Information

Classified National Security Information

The classification process is based on requirements set forth in a Presidential Executive Order. The current Executive Order governing the classification system is Executive Order 12958, as amended, "Classified National Security Information," March 2003 (hereafter referred to as the "Order"). The Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. The Order also assigns responsibility for implementation of the classified national security information program, in consultation with the Assistant to the President for National Security Affairs, to the Information Security Oversight Office (ISOO). In fulfilling this responsibility, ISOO publishes program regulations and directives for implementation of the Order. One such regulation is 32 CFR Part 2001/2004, "Classified National Security Information Directive No. 1." ISOO Directive No. 1 further defines and interprets the requirements set forth in the Order and provides instructions on implementation and management of a classification management program.

Additionally, the basis for determining eligibility for access to classified information is also governed by Presidential Executive Order and is set forth in Executive Order 12968, "Access to Classified Information."

What is Classified National Security Information?

Classified information is information that has been determined by a delegated official within the Executive Branch of the Federal Government to require protection because its release or disclosure could cause damage to the national security. Delegated officials make a determination on classification based on the standards and criteria cited in the Order.

Classification Levels

When a determination is made that information will be classified it is assigned one of three levels of classification. The level assigned is based on the potential damage to national security that could result should the information be released. The three levels of classification and their definitions are:

- **TOP SECRET** - information which, if disclosed without authorization, could reasonably be expected to cause ***exceptionally grave*** damage to the national security.
- **SECRET** - information which, if disclosed without authorization, could reasonably be expected to cause ***serious*** damage to the national security.
- **CONFIDENTIAL** - information which, if disclosed without authorization, could reasonably be expected to cause ***damage*** to the national security.

Other terms or phrases, such as ''Secret *Sensitive*,'' ''*Agency* Confidential,'' "*Colorado* Secret," "*New York* Confidential," "*Law Enforcement* Secret," etc., shall NOT be used in conjunction with the classification levels above to identify classified national security information. Although the use of such markings may reflect a level of sensitivity applicable within the respective jurisdiction, information that is marked in such a manner shall not fall under the purview of the Order and thus shall not be treated in the same manner or be afforded the same legal protections afforded

classified national security information. Where feasible, when non-Federal entities communicate with Federal agencies the use of "CONFIDENTIAL," "SECRET," and "TOP SECRET," in association with other locally established descriptors should be eliminated in order to avoid confusion.

What is not Classified National Security Information?

In addition to knowing what classified information is, it is also important to know what is not, and should not, be considered or referred to as classified information. The following are examples of various caveats used by different government agencies to denote information that is considered "sensitive" but unclassified:

- For Official Use Only (FOUO)
- Limited Official Use (LOU)
- Official Use Only (OUO)
- Law Enforcement Sensitive (LES)
- Sensitive Security Information (SSI)
- Protected Critical Infrastructure Information (PCII)
- And other caveats used to identify and categorize information as sensitive, but unclassified.

These categories of information are considered sensitive and do require a "need-to-know" for access as well as protection against unauthorized disclosure; but, they do not meet the standards for classification and thus, do not fall within the purview of the classification system. More information on sensitive but unclassified information is provided in Section II beginning on Page 25 of this booklet.

How Information Becomes "Classified" Information

The Order sets U.S. Government policy for properly classifying national security information that must be protected from unauthorized disclosure. Information is classified by one of two methods -- ORIGINAL classification or DERIVATIVE classification.

Original classification is the **initial** determination that information meets the standards and criteria for classification and requires protection against unauthorized disclosure. Only U.S. Government officials to whom this authority has been delegated in writing and who have been trained in classification requirements have the authority to originally classify information in the first instance. These officials are referred to as "Original Classification Authorities" (OCA's). Only appropriately delegated OCA's are authorized to perform original classification actions.

Derivative classification is the process whereby classified information is extracted from an existing classified source, such as a document, or a Security Classification Guide approved and published by an authorized original classification authority, and used in a newly created document. The person performing the derivative classification action derives, or carries forward the classification instructions from the source document to the newly created document. Therefore, the authority to classify the information is based on the existing classified source or guide. State, Local, Tribal, and Private Sector personnel

will not normally be called upon to perform derivative classification actions. However, should a need arise to do this, you must first contact the DHS Office of Security, Administrative Security Division (DHS OS/ASD).

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. Each classified document must be marked with specific classification markings to reflect the level of classification, the source (authority) of classification, and when the information can be declassified.

Sample Classified Document Markings

An example of a derivatively classified document with the appropriate classification markings and an explanation of those markings is provided below.

Portion Markings

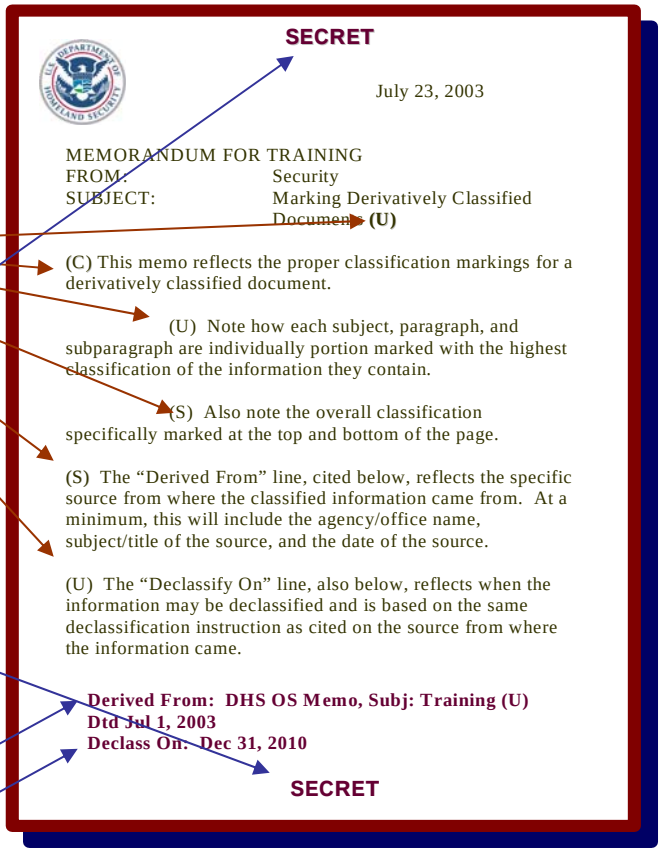
- Portion Markings are placed at the beginning or at the end of each title, subject, paragraph, subparagraph, or similar entity. The portion markings should be in parentheses and reflect the highest classification of the information within the portion.
    - (TS) TOP SECRET
    - (S) SECRET
    - (C) CONFIDENTIAL
    - (FOUO) FOR OFFICIAL USE ONLY
    - (U) UNCLASSIFIED

Overall Page Markings

- These markings are placed prominently and conspicuously at the top and bottom of each page and reflect the highest classification of information on the page or in the entire document.

Classification Actions

- The classification actions marking reflect the authority for the information to be classified and when the information can be declassified.
    - "Derived From" identifies the source from where the authority for classification came.
    - "Declass On" identifies a date or specific event in which the information can be declassified. In some cases, instead of a date you may see a marking such as X-1 or "Source Marked X-1, Date of Source (MMDDYYYY);" or, OADR or "Source Marked OADR, Date of Source (MMDDYYY)." These markings mean the information will not be declassified on a specific date and will retain its classification until determined otherwise by an authorized official.



Additional Control Markings

Additional Control Markings are "caveats" prescribed by Director Central Intelligence Directive (DCID) 6/6, "Security Controls on the Dissemination of Intelligence Information," and other DCID's, as a means to further restrict or control access to certain types of information. Control markings are not classifications. They are used in conjunction with, not in lieu of, the appropriate classification levels of CONFIDENTIAL, SECRET, or TOP SECRET. Although you may not encounter caveated information, below are examples of the most common caveats so that should you see them you will recognize them and understand their meaning:

- **NOFORN** - stands for "Not Releasable to Foreign Nationals." Information that has been additionally marked with the NOFORN caveat may not be provided, in any form, to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens. The parenthetical marking for this caveat is (NF).

- **PROPIN** - stands for "Caution – Proprietary Information Involved." The PROPIN control marking can be used with or without a security classification level. It is used to identify information provided by a commercial firm or private source with the understanding that the information will be protected. The parenthetical marking for this caveat is (PR).

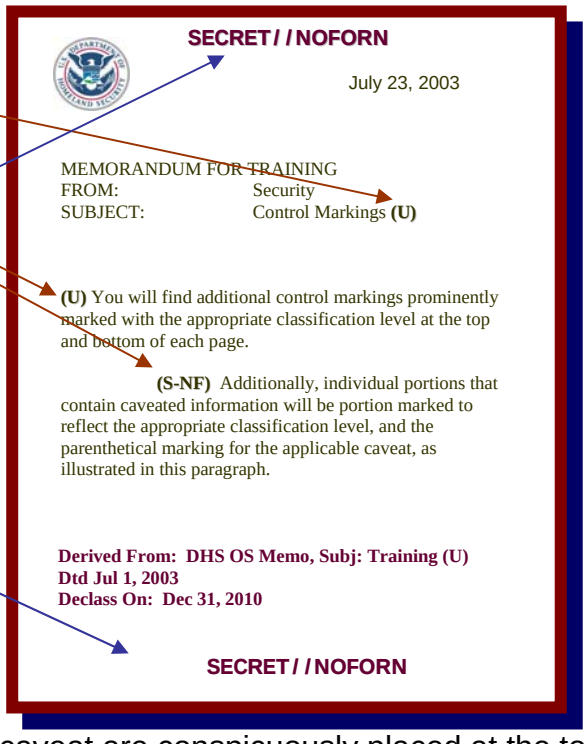
- **ORCON** - "Dissemination and Extraction of Information Controlled By Originator." This is the most restrictive of control markings and indicates that under no circumstances shall you further disseminate the marked information without prior approval of the originator. The parenthetical marking for this caveat is (OC).

Portion Markings

Each paragraph, subparagraph and similar portion will be parenthetically marked with the highest classification of the information contained within the portion, as well as, the parenthetical marking for the applicable caveat. In this instance, this particular paragraph contains SECRET information that is "Not Releasable to Foreign Nationals."

Overall Page Markings

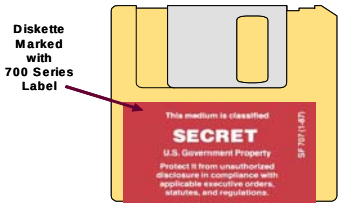
This identifies the highest classification level of information contained in the document, and, where applicable, the appropriate caveat. In this case, the document contains information that the originator has determined is "Not Releasable to Foreign Nationals." Therefore, the overall page marking reflects that, in addition to the information being classified at the SECRET level, it is also not to be released to foreign nationals. The overall classification and the applicable caveat are 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, and, the applicable caveat.



Marking Classified Diskettes and Other Media

In some cases equipment may be deployed to State, Local, Tribal, or Private Sector entities that will allow for connectivity to a classified network, thereby allowing for access to classified information resident on the network. In such cases, all equipment, e.g., diskettes, computers, laptops, removable hard drives, 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.

TOP SECRET
SF 706



SECRET
SF 707

CONFIDENTIAL
SF 708

UNCLASSIFIED
SF 710

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 Federal government official. Contact the DHS OS/ASD for additional information.

Access to Classified Information

No person shall be given access to classified information unless it has been properly verified that the intended recipient has been granted a security clearance by an authorized agency of the Federal government, at a level equal to or higher than the level of classified information to which access will be given.

No person is authorized access to classified information simply by virtue of their rank, title, or position.

Prior to an individual being given access to classified information, three conditions must be met:

1. Personnel shall have been subjected to a background investigation and the completed background investigation must have been favorably adjudicated and a security clearance issued by an authorized Federal agency. Verification of a persons' security clearance must be in the form of written documentation provided by the Federal agency that granted the security clearance.

2. A Standard Form 312, Classified Information Nondisclosure Agreement, has been signed and accepted by an appropriate Federal Government official. The assumption can be made that if a Federal agency has granted a person a security clearance, that person has executed a SF 312 as part of the clearance process.

3. There must be a demonstrated need-to-know.

Need-to-Know

"Need-to-Know is the determination made by an authorized holder of classified information that access to the information is required by another appropriately cleared individual in order to perform official duties."

Your security clearance does not give you approved access to all classified information. In addition to a security clearance, an individual must have a "need-to-know" before being given access to information.

 **Need-to-know is one of the most fundamental security principles. The practice of need-to-know limits the damage that can be done by a trusted insider who goes bad. Failures in implementing the need-to-know principle have contributed greatly to the damage caused by a number of recent espionage cases.**

Need-to-know imposes a dual responsibility on you and all other authorized holders of classified information:

- When doing your job, you are expected to limit your requests for information to that which you have a genuine need-to-know. Under some circumstances, you may be expected to explain and justify your need-to-know when asking others for information.
- Conversely, you must ensure that anyone to whom you give classified information has a legitimate need to know and the appropriate clearance to receive that information. You are obliged to ask the other person for sufficient information to enable you to make an informed decision about their need-to-know, and the other person is obliged to justify their need-to-know. In situations where there is uncertainty as to whether a person has a need-to-know, you should contact the originator of the information for clarification or consult with the DHS OS/ASD.

The need-to-know principal is sometimes difficult to adhere to as it conflicts with our natural desire to be friendly and helpful. However, its' importance can not be overstated and each person with access to classified information must maintain a level of self-discipline and responsibility in ensuring it is a principal we abide by. Here are some specific circumstances when you need to be particularly careful:

- An individual from another organization may contact you and ask for information about classified information you have in your possession. Even though you have confirmation that the person has the appropriate level security clearance, you are also obliged to confirm the individual's need-to-know before providing information. If you have any doubt, contact the information's originator or consult with the DHS OS/ASD.
- Difficult situations sometimes arise when talking with friends who used to be assigned to the same classified program where you are now working. The fact that a colleague formerly had a need-to-know about this program does not mean he or she may have access to the information. There is no "need" to keep up to date on sensitive developments after being transferred to a different assignment.

Granting a Security Clearance

The sanctity of the classification program is dependent upon the suitability, integrity, trustworthiness, and reliability of the persons to whom access to classified information is granted. As such, prior to being granted access to classified information each person must be subjected to a background investigation, the results of the background investigation must be favorably adjudicated based on Federal adjudicative standards, and the security clearance formally issued to those persons deemed worthy of such trust. The level of security clearance granted, CONFIDENTIAL, SECRET, or TOP SECRET, is normally dependent upon the associated level of classified information a person will require access too and the favorable adjudication of an appropriate background investigation. The granting of a security clearance is a privilege – not a right.

The granting of a security clearance by DHS to State, Local, Tribal, and Private Sector personnel will be limited to the SECRET level and based on a justified need that the person to whom the clearance is to be granted requires or will require access to classified information. When justified and when in support of the DHS mission, DHS will sponsor the initial granting of a security clearance to those personnel who currently do not have one. Contact your State Homeland Security Advisor or Private Sector representative for additional guidance.

If a person currently holds a security clearance granted by another Federal agency and requires access to classified information in support of the DHS mission then the security clearance granted by the other agency should be reciprocally transferred to DHS usually without the need for a new investigation. By doing so, DHS will simultaneously hold your clearance in conjunction with your original sponsoring agency. Holding a DHS-sponsored clearance provides a number of advantages to DHS as well as to State, Local and Private Sector personnel. This will allow the Department to provide you access to DHS classified meetings, equipment and systems at your appropriate clearance level without requiring yearly re-certification of your clearance status from your sponsoring agency. It will also reduce the vulnerability of inadvertent disclosures or compromise of classified information. Contact your State Homeland Security Advisor or Private Sector representative for additional guidance.

Classified Discussions and Meetings

Special care must be taken when discussing classified information in the workplace. The capability and the authority to have classified discussions within facilities under the jurisdiction of State, Local, Tribal, and Private Sector entities is strictly limited to rooms/areas that have been subjected to a survey by appropriate Federal authorities. For example, a private office that has been surveyed and approved by a Federal authority for the installation of a secure telephone can of course be used for classified discussion. However, when classified discussions occur either through the use of secure telephone or in face to face meetings, it is incumbent upon the participants to:

- Ensure the security clearances of participants are at least equal to the level of classified information to be discussed.
- Ensure all electronic equipment maintained in the room that is capable of transmitting signals outside the room is powered off, i.e., cell phones, PDAs, and blackberries.
- Ensure normal conversation taking place inside the room/area can not be heard outside of the room/area.

- If necessary, 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.
- Prohibit those without proper authorization and clearance from participating.
- Notify participants of the highest level of classified information to be discussed.
- Comply with all security safeguards for classified information.

Formal group meetings and other gatherings that will include classified discussions shall be conducted only at U.S. Government owned facilities or at contractor facilities that have been cleared under the National Industrial Security Program. Contact DHS OS/ASD for additional guidance.

NOTE: Classified information must not be discussed in any public area, such as in restaurants, hallways, elevators, etc., on any public or private conveyance, such as a train, plane, bus, car, etc., or in any other area where uncleared persons and/or persons without a need-to-know may overhear the discussion.

Handling Classified Information

As an approved custodian or user of classified information, you are personally responsible for the protection and control of this information. You must safeguard this information at all times to prevent loss or compromise and unauthorized disclosure, dissemination, or duplication. Unauthorized disclosure of classified information can be punishable under Federal Criminal Statutes or, at a minimum, administrative sanctions – to include revocation of a security clearance.

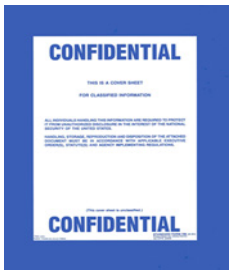
Classified information that is not stored in an approved security container (See Page 13) shall be under the constant control of a person having the proper security clearance and need-to-know. An end-of-day security check must be in place at all locations where classified information is stored or where classified equipment, such as a secure telephone, is deployed. See "End of Day Security Checks" on Page 14.

Classified information shall not be taken home under any circumstances.

Classified Cover Sheets

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

SF 703-TOP SECRET **SF 704-SECRET** **SF 705-CONFIDENTIAL**



Classified information shall not be disposed of in a waste basket or recycling bin. It must be placed in a safe approved for classified storage, or destroyed in a manner authorized for the destruction of classified material. See "Destruction of Classified Materials" on Page 18.

All forms associated with the safeguarding of classified information, i.e., cover sheets, destruction certificates, etc., can be obtained by contacting DHS OS/ASD.

Storing Classified Information

When not under the personal control of an authorized person, classified information must be stored in an approved security container. The equipment required for the storage of classified information is as follows:

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 or CONFIDENTIAL must be stored in a GSA approved container bearing the GSA approved label. No supplemental controls are necessary.

Security containers used for the storage of classified information shall be placed in a room or area where access is restricted to a limited number of personnel.

Collateral Open Storage Area

When equipment is deployed that allows for connectivity to an external network that affords access to classified information, for example, the Homeland Security Data Network (HSDN) or the Homeland Security Information Network −SECRET Level (HSIN-S) the room/area where the equipment is deployed shall be built to the standards of and approved as an "Open Storage Area." Such rooms/areas shall be constructed in accordance with DHS Management Directive (MD) Number 11046, "Open Storage Area Standards for Collateral Classified Information," and authorized in writing by DHS OS/ASD. Contact DHS OS/ASD for standards, specifications, and procedures for open storage of classified information. See the State, Local and Private Sector Security Matrix as a reference for safeguarding and storage standards (Matrix Attached).

In certain circumstances, such as JRIES-S deployment through the Critical Infrastructure Warning Information Network (CWIN), a security container may be used in lieu of an open storage area for the storage of equipment associated with the CWIN classified connectivity. In this specific instance and based on the appropriate configuration, classified connectivity is terminated and can not be restored once the cryptological key (encryption device) is removed from the equipment and the equipment is severed from CWIN.

In this case, all associated equipment can then be stored in a GSA Approved container without the need for an approved open storage area. However, JRIES-S/CWIN must be activated only in a room/area equipped with a lockable door and where access is restricted to only cleared personnel. Contact DHS OS/ASD for additional guidance.

Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas

The combination to containers used for the storage of classified information are themselves classified at the highest level of the information stored therein and must be protected accordingly.

Only a minimum number of authorized persons with the appropriate level security clearance shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage. Combinations will be annotated on a Standard Form 700 (SF 700), "Security Container Information," and the DHS OS/ASD will be contacted for additional guidance on the appropriate location and methods to store the completed form. The SF 700 will not be stored in the same safe that bears the combination. Combinations shall not be written down in any other manner and storage of a combination outside of an approved storage location constitutes a security violation.

A record of the names of persons having knowledge of the combinations shall be maintained.

Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person.

The combination shall be safeguarded and marked in accordance with the highest classification of the material authorized for storage in the container. Superseded combinations shall be destroyed.

Changing Combinations

Combinations are to be changed by persons having an appropriate security clearance, who are authorized access to the contents of the container, and who have received instructions on how to change them. Contact DHS OS/ASD when assistance or guidance is needed.

Combinations shall be changed as follows:

- When an approved container is first placed in use for the storage of classified material.
- Upon termination of employment or reassignment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.
- Upon compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.
- At least every two years

End of Day Security Checks

Rooms/areas that store classified information shall establish a system of security checks at the close of each working day to ensure that all classified information and security containers have been appropriately secured.

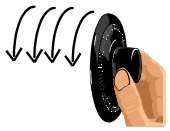
Facilities that operate multiple work shifts shall perform the security checks at the end of the last working shift in which classified information had been removed from storage for use. The checks are not required during continuous 24-hour operations.

End of Day Security Checks will be conducted by a person who has been granted a security clearance and will be recorded on a SF 701, Activity Security Checklist (Form Attached). The SF 701 can be maintained anywhere within the applicable room/area where the classified information is stored but is often posted in the immediate vicinity of the room/area exit for convenience and to serve as a reminder to the checker.

Additionally, the opening and closing of individual safes will be recorded on a SF 702, Security Container Check Sheet, (Form Attached). The SF 702 will be used to record the date, time, and initials each time an individual safe is opened, closed, and checked

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 they 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/wastebaskets for the presence of classified materials.
- ✓ Visually inspect copiers, fax machines, and printers to ensure there are no classified materials in, on, or near the devices.
- ✓ Check other items/devices as deemed necessary for your particular office/work area.

Mailing Classified Information

Although there should be limited circumstances where you would have a need to send classified information through the mail, should the need arise, the following applies:

TOP SECRET material shall NOT be sent through the mail under any circumstances. It must be transmitted by cleared courier or approved electronic means. Contact DHS OS/ASD.

SECRET or CONFIDENTIAL information may be transmitted by US Postal Service Registered Mail, or US Postal Service Express Mail. When using US Postal Service Express Mail, Item 11B of the Express Mail transmittal form, "Waiver of Signature Indemnity," must not be completed. The use of external (street side) express mail collection boxes is prohibited. A document receipt, DHS Classified Document Record, will be prepared by the sender and attached to the document. See DHS Classified Document Record (Form Attached). The purpose of the receipt is to ensure the intended recipient receives the materials sent to them. Upon receipt, the intended recipient shall acknowledge receipt by signing the receipt form and sending it back to the sender. The sender will retain the signed receipt on file for two years. If the sender does not receive a signed receipt back from the intended recipient within 20 work days of shipment, the sender will initiate a tracer to determine the disposition of the sent materials. Contact DHS OS/ASD for assistance.

Classified information transmitted outside a facility, whether by mail or hand-carried, will be double wrapped as explained on Page 16.

Note: Classified information shall not be sent through an inter-office distribution system.

Carrying Classified Information Inside the Building

When carrying classified information internally within a building but outside of the room in which it is stored, the materials will be covered by the appropriate cover sheet and placed in an unmarked envelope or folder so as not to draw undue attention to the material.

Carrying Classified Information Outside of a Building

Personnel that have a justified need to hand-carry classified information outside of the building where the information is stored are to request approval from DHS OS/ASD, and receive a classified courier briefing. Classified information shall not be hand-carried outside of a building unless the person hand-carrying the information has received a classified courier briefing and been issued a classified courier authorization card. Classified information hand-carried outside of a building will be double wrapped as explained on the following pages.

DHS Courier Cards are issued on a limited basis to individuals to whom DHS has granted a security clearance or whose security clearance has been reciprocally transferred to DHS from another agency. To request a DHS courier card, submit a DHS Form 11000-02, Courier Authorization Request (Form Attached), to DHS OS/ASD.

DHS Courier cards are issued for local metropolitan commuting areas in support of DHS related classified activities. In conjunction with the courier card the bearer, upon request, will present an official government issued photo identification or credential to verify identity.

In the rare occurrence that a need arises to transport classified materials aboard a commercial aircraft, prior approval must be obtained from DHS OS/ASD. Before approval is granted, the requester must provide sufficient justification as to why the materials must be hand-carried versus the use of other approved means, such as US Postal Service Registered Mail for SECRET and CONFIDENTIAL materials.

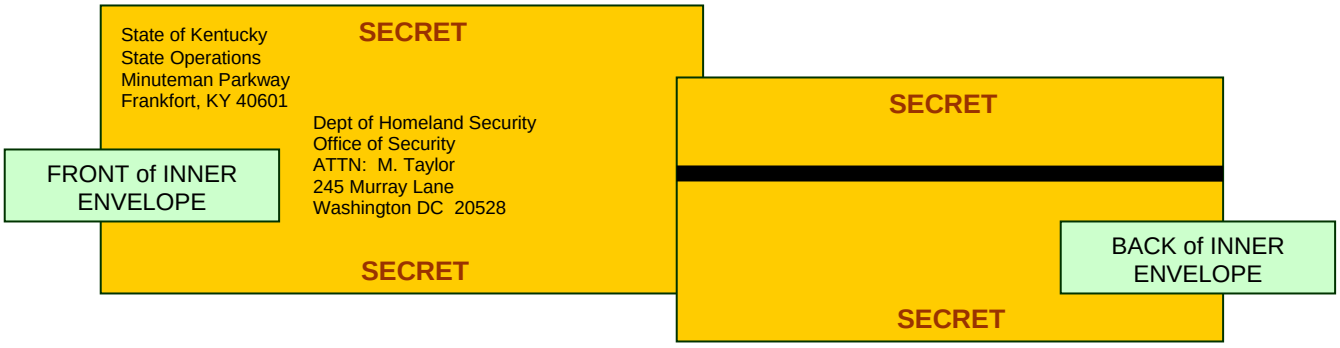
Individuals nominated and approved by DHS OS/ASD as classified couriers will be provided with specific information on their duties and responsibilities and must sign a briefing acknowledgement form prior to being issued a courier card.

Wrapping

All classified material must be double-wrapped with opaque inner and outer covers when transporting outside of a building or sending through the mail. It shall be wrapped and marked as follows:

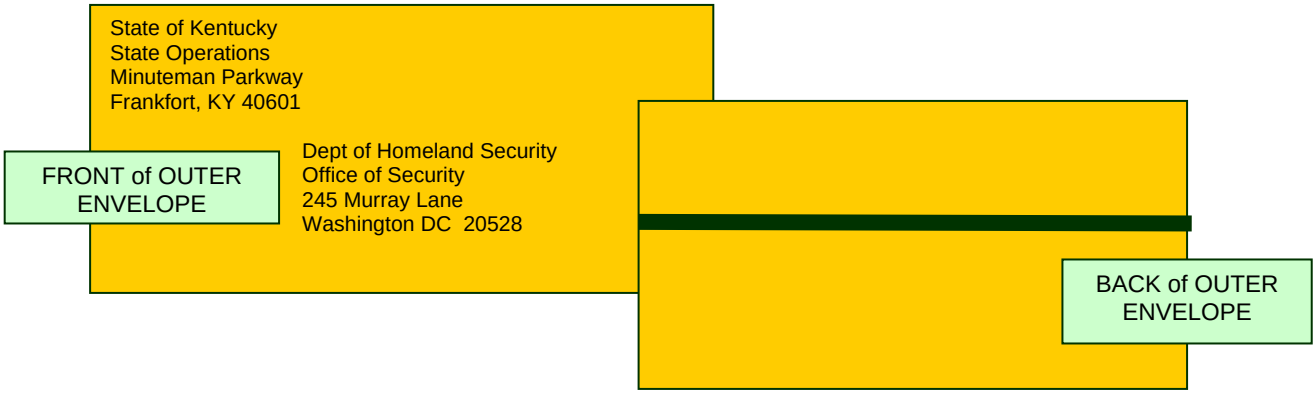
Inner Envelope

- Prominently and conspicuously mark the inner envelope top and bottom on both sides, preferably in red, with the highest classification of the materials being transmitted.
- Write the complete mailing address and complete return address on the inner envelope. The address on the inner envelope should have the name of an appropriately cleared individual.
- Seal the envelope with reinforced tape to prevent inadvertent opening and show evidence of tampering.



Outer Envelope

- Write the complete mailing address and complete return address. However, do not include personal names on the outer envelope. Instead, in an "Attention" line identify the organization, office code, office symbol, etc., of the intended recipient.
- **DO NOT PLACE ANY CLASSIFICATION MARKINGS ON THE "OUTER" ENVELOPE.**
- As a reminder SECRET and CONFIDENTIAL information is required to be mailed via US Postal Service Registered or US Postal Service Express Mail



Reproduction of Classified Materials

Prior authorization must be received from DHS OS/ASD, before making copies of classified information.

The following guidelines govern the reproduction of classified information:

- Reproduction of classified will be kept to an absolute minimum, consistent with operational requirements. Classified information in your possession is not to be copied without prior approval from DHS OS/ASD. Approval will be granted based on need and justification as well as identification of the intended recipients.
- Honor any reproduction restrictions cited and where there is uncertainty over the authority to reproduce contact the originator for approval.
- Reproduction must not be done on machines connected to an unclassified LAN or remote diagnostics or on machines equipped with a hard-drive or other devices that 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 of the classified paper products you will encounter can be destroyed using existing cross-cut shredders with the particle size of the cuts not exceeding 1/32 X 1/2 inch, provided the bag contents are stirred prior to disposal and unclassified paper products are also shredded and mixed in with the classified products. However, certain types of classified information, for example; Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) paper products, require more stringent destruction standards. Newly purchased or replacement shredders and shredders that will be used for the destruction of SCI and COMSEC paper products, shall conform to the more stringent standard. Contact DHS OS/ASD, or go to http://www.nsa.gov/ia/government/mdg.cfm?MenuID=10.3.1, *NSA/CSS Evaluated Products List (EPL) for High Security Crosscut Paper Shredders*, for information on approved shredders.

Two cleared people must be involved in the destruction of TOP SECRET materials - one to destroy and one to witness the destruction. A Certificate of Destruction, DHS Classified Document Record (Form Attached) will be used to record the destruction.

One cleared person can destroy SECRET and CONFIDENTIAL. A destruction certificate is not required unless required by the originator.

Appropriate Use Of Computer Systems

Misuse of an automated information system is sometimes illegal, often unethical, and always reflects poor judgment or lack of care in following security rules and regulations. Misuse may, unintentionally, create security vulnerabilities or cause leaks of important information. A pattern of inability or unwillingness to follow rules for the operation of computer systems raises serious concerns about an individual's reliability and trustworthiness.

Security Rules

The following are basic rules for secure use of a computer.

- Do not access any computer system without authorization. Unauthorized access to a protected or compartmented computer file is a serious security violation. It can be a basis for revocation of your security clearance. Whether motivated by the challenge of penetrating the system or by simple curiosity to see what is there, unauthorized access is a deliberate disregard for rules and regulations. It can cause you to be suspected of espionage. At a minimum, it violates the need-to-know principle and in some cases is an invasion of privacy.
- ***Do not store or process classified information on any system not explicitly approved for classified processing by an appropriate Federal government official.***
- Do not attempt to circumvent or defeat security or auditing systems without prior authorization from the system administrator, other than as part of a system test or security research authorized in advance.
- Do not use another individual’s user ID, password, or identity.

- Do not permit an unauthorized individual (including spouse, relative, or friend) access to any sensitive computer network.
- If you are the inadvertent recipient of classified material sent via e-mail or become aware of classified material on an open bulletin board or web site, report it to DHS OS/ASD via secure means.

Security Risks with E-Mail

Classified information must not be sent via an unclassified email system or in any way posted on any internet, intra-net, virtual private network, or any other automated communications tool that has not been specifically approved for processing classified information.

E-mail and the internet create many opportunities for inadvertent disclosure of classified information. Before sending an e-mail, posting to a bulletin board, publishing anything on the internet, or adding to an existing Web page, you must be *absolutely* certain none of the information is classified or sensitive unclassified information.

As a result of the internet and e-mail, there has been a sharp increase in security incidents involving the accidental disclosure of classified and other sensitive information. One common problem occurs when individuals download a seemingly unclassified file from a classified system, and then fail to carefully review this file before sending it as an attachment to an e-mail message. Too often, the seemingly unclassified file actually has some classified material or classification markings that are not readily apparent when the file is viewed on line. Sending such material by e-mail is a security violation even if the recipient has an appropriate security clearance, as e-mail can easily be monitored by unauthorized persons.

More important, even if the downloaded file really is unclassified, the electronic version of that file may have recoverable traces of classified information. This happens because data is stored in "blocks." If a file does not take up an entire block, the remainder of that block may have recoverable traces of data from other files. An approved technical procedure must be followed for removing these traces before the file can be treated as unclassified.

Telephone Use and Classified Conversations

Classified information must not be discussed over non-secure telephones. Never attempt to talk around classified information over an unsecured telephone system. Classified telephone discussions must be conducted using secure equipment, i.e., 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 need-to-know for the information being discussed. The discussion cannot exceed the level of classification for which the STU-III/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.

Secure Telephone Unit III (STU-III) & Secure Terminal Equipment (STE) Security Guidance

There are two types of secure telephone devices that, when appropriately configured, allow for the telephonic discussion of classified information. The two types of telephones are the older generation Secure Telephone Unit III (STU-III) and the next generation, Secure Telephone Equipment (STE). The following provides some brief information and guidance on the use of each of them.

The STU-III and STE are two-part systems. The STU-III instrument – which is the telephone itself, is one part and the associated Crypto Ignition Key (CIK) is the second part. For the STE, the instrument (telephone) is the one part and its associated Fortezza+ Crypto Card (KOV) is the second part. The STU-III/STE instruments standing alone without the associated CIK/KOV inserted are considered "Controlled Cryptographic Items" (CCI) that require the same level of protection you would afford a high value item. CCI equipment must be protected in a manner that provides sufficient protection to preclude theft, sabotage, tampering, and unauthorized access.

However, when the CIK/KOV are inserted into the instruments, then the instrument takes on the same level of classification for which the CIK/KOV have been programmed and therefore require the same level of protection associated with that level of classification.

The STU-III/STE instrument may be installed and used in any room in which classified conversations are permitted. Once installed – it must not be moved from that location without prior coordination and approval of your Federal COMSEC Custodian. The COMSEC Custodian is the authorized individual responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a particular COMSEC account.

Each STU-III/STE terminal has a two-line display that prompts the user through the various phases of a call and other terminal operations. When a user calls another STU-III/STE terminal, the terminals communicate with each other during the secure mode setup. Each terminal automatically displays authentication information of the distant terminal.

Each user is responsible to observe the terminal display before communicating any classified information, either voice or data. The classification level displayed will be the highest common level shared by the two terminals for that call. The terminal user should restrict the classification level of the conversation (or data traffic) to no higher than the displayed level.

The information displayed indicates the approved clearance level for that call, but does not authenticate the person using the terminal. Therefore, users must use judgment in determining need-to-know when communicating any classified information.

- STU-III/STE telephones deployed to State, Local, Tribal and Private Sector customers are keyed to and authorized for use at the SECRET level.
- Locations where a STU-IIIs and STEs are deployed shall have a GSA Approved container available for the storage of the CIK/KOV. When unattended, the CIK/KOV shall be stored in the approved container.
- When accountable COMSEC material is to be issued to a user, the authorized COMSEC Custodian will issue the material on a Hand Receipt in the form of an SF-153, COMSEC Material Report. **Hand Receipt users are not authorized to reissue the material and must report the intention to move the equipment prior to taking action. Only a COMSEC Custodian can issue a hand-receipt or authorize moving equipment.**

- Individuals with an Interim SECRET clearance may have access and may use the phone, but the STU-III/STE can only be deployed where an individual with a Final SECRET clearance or higher can take responsibility for it/them.

Faxing Classified Information

Classified materials must not be transmitted over any fax machines that have not been approved specifically for that purpose. Contact DHS OS/ASD for fax machines approved for classified transmittal. A justification is required with your request for approval to use a secure fax. When activated to receive, approved secure fax machines will be under the constant surveillance of cleared personnel unless the room/area in which the secure fax resides has been approved for open storage by DHS OS/ASD or another Federal agency.

Reportable COMSEC Incidents

With any secure communications system, insecurities and compromises of terminals and keys are possible. The design of the STU-III/STE terminals minimizes the threat of compromised communications. The following incidents are to be reported immediately to the COMSEC Custodian:

- Loss of any CIK/KOV card must be promptly reported to your local supporting COMSEC custodian/alternate so the key or card can be deleted from the respective terminal. (If a CIK/KOV is broken or damaged it should be returned to the local COMSEC custodian for replacement.)
- Loss or missing STU or STE terminal.
- Leaving the CIK/KOV in a terminal when the terminal is unattended and in a nonsecure area.
- Using a STU-III/STE terminal in the secure mode when the visual display in inoperable.
- Indication in the terminal's display that the distant terminal contains compromised key.
- Failure to rekey a terminal within two months of the end of the cryptoperiod.
- Failure to adequately protect or zeroize a CIK/KOV that is associated with an unkeyed terminal which is lost.

Security Violations

A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results. No matter how seemingly minor, any security infraction or violation must be reported immediately to DHS OS/ASD, so that the incident may be evaluated and any appropriate action taken.

The following are examples of security violations:

- Leaving a classified file or security container unlocked and unattended either during or after normal working hours.
- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.

- Reproducing or transmitting classified material without proper authorization.
- Removing classified material from the work area in order to work on it at home.
- Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know.
- Discussing classified information over the telephone, other than a phone approved for classified discussion.
- Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard.
- Carrying safe combinations or classified computer passwords (identifiable as such) on one's person, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computer.
- Failure to mark classified documents properly.
- Failure to follow appropriate procedures for destruction of classified material.

Major Violations

The significance of a security violation does not always depend upon whether information was actually compromised. It may also depend on the intentions and attitudes of the individual who committed the violation. The ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining your security clearance. Although accidental and infrequent minor violations are to be expected, deliberate or repeated failure to follow the rules is definitely not. It may be a symptom of underlying attitudes, emotional, or personality problems that are a serious security concern.

The following behaviors are of particular concern and may affect your security clearance:

- A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline.
- Taking classified information home, or carrying it while in a travel status without proper authorization.
- Being intoxicated while carrying classified materials which could cause one to speak inappropriately about classified matters to unauthorized persons.
- Deliberate revelation of classified information to unauthorized persons to impress them with one's importance.
- Copying classified information in a manner designed to obscure classification markings. This may indicate intent to misuse classified information.
- Making unauthorized or excessive copies of classified material. Going to another office to copy classified material when copier equipment is available in one’s own work area is a potential indicator of unauthorized copies being made.
- Failing to report requests for classified information from unauthorized individuals.

Failure to report a security violation is itself a security violation and may be a very serious concern. After the arrest of Navy spy Jerry Whitworth, who was part of the infamous John Walker spy ring, interviews with Whitworth's work colleagues identified one who had noticed classified papers in Whitworth's personal locker, another who had observed Whitworth monitoring and copying a sensitive communications line without authorization, and a third who knew Whitworth took classified materials home with him but believed he was doing it only to keep his work current. Failure to report these violations enabled Whitworth's espionage to continue.

Possessing classified information in the home is a very serious concern as it may indicate current or the potential for future espionage. At the time of their arrest, many well-known spies were found to have large quantities of classified documents at their residences. CIA spy Aldrich Ames had 144 classified documents at his home, while Edward Moore had 10 boxes of documents at home. Of various Navy spies, Jonathan Pollard had a suitcase full of classified materials, Michael Walker had 15 pounds of classified material, while Samuel Morison had two portions of Navy documents marked SECRET.

Sanctions

Violations of policy for the safeguarding of classified information could result in a number of actions, both civil and criminal. Among the civil actions that the Government may bring in Federal court are the application for a court order enjoining the publication or other disclosure of classified information; suits for money damages to recompense the United States for the damages caused by an unauthorized disclosure; and suits to require the forfeiture to the United States of any payments or other monetary or property gains that have resulted or may result from an unauthorized disclosure.

The scope of prospective administrative actions depends on whether the person alleged to have violated the terms of the SF 312, Classified Information Nondisclosure Agreement, is a Government or non-Government employee. A Government employee would be subject to the entire range of administrative sanctions and penalties, including reprimand, suspension, demotion or removal, in addition to the likely loss of the security clearance.

In situations involving an unauthorized disclosure by a non-Government employee, the action will focus on the relationship between the Government and the organization that employs the individual. The Government cannot remove or otherwise discipline a non-Government employee, but it can, and in all likelihood will revoke the security clearance of that employee, and prevent the employing organization from using that employee on classified projects. The Government may also move against the employing organization in accordance with the terms of their relationship.

TEN POINTS TO KEEP IN MIND…

1. By signing an SF 312, “Classified Information Nondisclosure Agreement,” you are contractually obligated to the US Government to safeguard classified information.

2. Access to classified information requires both a security clearance and a “Need-to-Know.” No one is authorized access to classified information strictly by virtue of their rank, title or position.

3. When not under the direct control of an authorized person, classified information must be stored in an approved container.

4. Never discuss classified information over an unsecure telephone, in the presence of uncleared persons, or in public places, to include, restaurants, buses, trains, airplanes, unsecure office environment, etc.

5. Combinations to containers used for the storage of classified information are themselves classified at the same level as the information stored therein and must be protected accordingly.

6. Classified information is not to be copied without prior approval.

7. When carrying classified information within a building it will be placed in an unmarked envelope or folder so as not to draw attention to the content.

8. When carrying classified information outside of a building it must be marked and wrapped accordingly.

9. Never enter classified information into any automated system that has not been specifically approved for that purpose.

10. And finally…

WHEN IN DOUBT…CONTACT THE DHS OS/ASD
(202) 401-6173

SECTION II: Sensitive But Unclassified Information

For Official Use Only (FOUO)

FOUO is the marking used by DHS to identify Sensitive but Unclassified information within the DHS community, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other operations essential to the national interest and that is not otherwise covered by a statute or regulation.

Other government agencies and international organizations frequently use different terms to identify sensitive information, such as "Limited Official Use (LOU)," "Official Use Only (OUO)," and in some instances "Law Enforcement Sensitive (LES)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO.

However, other agencies and international organizations may have additional requirements concerning the safeguarding of their sensitive information. When available, follow the safeguarding guidance provided by the other agency or organization. Should no guidance be available the information will be safeguarded in accordance with the FOUO guidance provided in this booklet.

It is not permitted to mark Information as FOUO to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency.

Marking

Information determined to be FOUO will be sufficiently marked so that persons granted access to it are aware of its sensitivity and protection requirements. At a minimum, it is marked on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO information can 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.

Markings typically associated with classified information such as originator information, downgrading instructions, and date/event markings are not required on FOUO documents.

Access and Dissemination

A security clearance is not needed for access to FOUO information. Access to FOUO information is based on a "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 should request dissemination instructions from their next-level supervisor or the originating activity.

FOUO information may be shared with other agencies, Federal, state, tribal, private sector, or local government and law enforcement officials, provided a need-to-know has been established and the information is shared in the furtherance of an official governmental activity, to include homeland defense, and no dissemination restrictions have been cited by the originator.

When discussing FOUO information over a telephone, use of the STU-III or 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 a recipient is present at

the time of the fax and that the materials faxed will not be left unattended or subject to unauthorized disclosure.

FOUO information may be transmitted over official 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.

Do not enter or post any FOUO information 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 shall 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

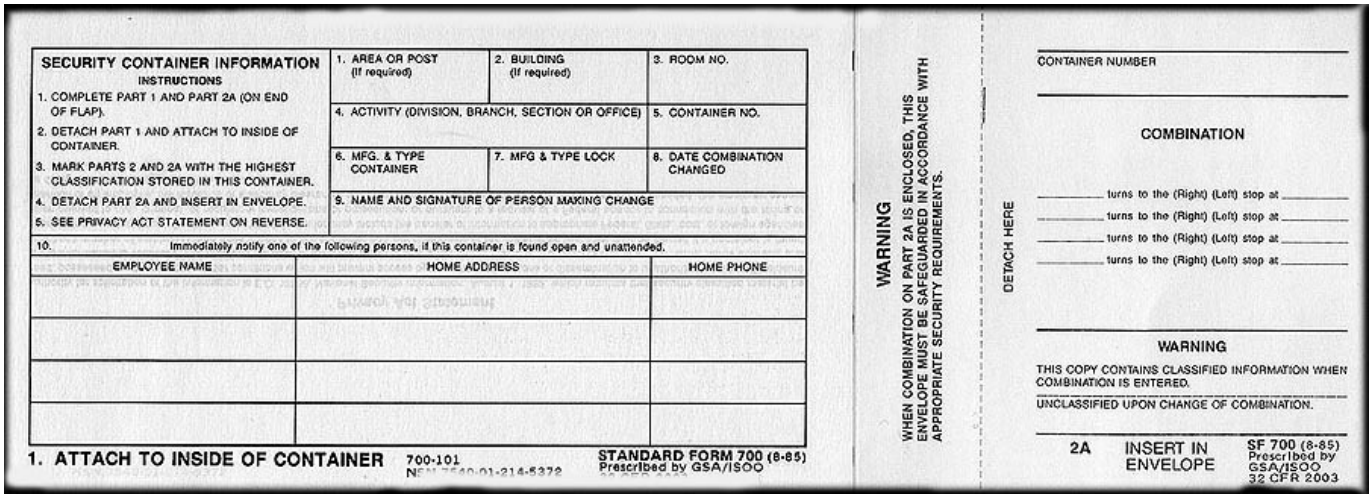
- Hard copy FOUO materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition and reconstruction.
- After destruction, materials may be disposed of with normal waste.
- Electronic storage media shall be sanitized appropriately by overwriting 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

- Compromise, suspected compromise and suspicious or inappropriate requests for FOUO information shall be reported to the originator of the information.
- Additional guidance or assistance can be obtained by contacting the DHS OS/ASD

ATTACHMENTS

Instructions for Completing Standard Form 700



SECURITY CONTAINER INFORMATION
INSTRUCTIONS
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required) | 2. BUILDING (If required) | 3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE) | 5. CONTAINER NO.
6. MFG. & TYPE CONTAINER | 7. MFG & TYPE LOCK | 8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE

10. Immediately notify one of the following persons, if this container is found open and unattended.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER 700-101 NSN 7540-01-214-5372 STANDARD FORM 700 (8-85) Prescribed by GSA/ISOO

WARNING
WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER

COMBINATION

_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____

WARNING
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.
UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A INSERT IN ENVELOPE SF 700 (8-85) Prescribed by GSA/ISOO 32 CFR 2003

Copy of Standard Form 700

It can be costly and time consuming when a GSA-approved security container or vault cannot be opened because the combination is lost or forgotten. Once a container or vault has been forcibly opened, the classified material must be safeguarded until the damaged container is repaired. The purpose of this form is to maintain a written record of the combination for use in just such circumstances, and, to identify contact information for persons responsible for the safe in the event an incident occurs – such as the safe is found open and unattended.

Details of the form:

The SF 700 comes in 3 parts:

Part 1-Fill out the information requested on Part 1. When completed, detach at the perforation from Part 2. Affix the detached Part 1 to the inside of the locking drawer of the safe. Part 1 is not classified as it does not contain the combination to the safe.

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. Contact DHS OS/ASD for storage instructions.

Why the form is needed:

The combination of a container, vault, or secure room used for the storage of classified information, shall be treated as information having a classification equal to the highest classification of the information stored therein. Any written record of the combination shall be marked with the appropriate classification level.

A record shall be maintained for each vault or secure room, door or container, used for storage of classified information. The location of the door or container, the names, home address and home telephone numbers of the individuals having knowledge of the combination who are to be contacted in the event the vault, secure room, or container is found open and unattended will be shown. Standard Form 700, "Security Container Information," shall be used for the purpose.

ACTIVITY SECURITY CHECKLIST	Division/Branch/Office:	Room Number:	Month/Year
Irregularities discovered will be promptly reported to the designated Security Office for corrective action.	Statement I have conducted a security inspection of this work area and checked all items listed below.		

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Security containers have been locked and checked																															
Desks, wastebaskets and other surfaces and receptacles are free of classified material .																															
Windows and doors have been locked (where appropriate)																															
Typewriter ribbons and ADP devices (e.g. disks, tapes) containing classified material have been removed and properly stored.																															
Security alarm(s) and equipment are activated where appropriate																															
INITIAL FOR DAILY REPORT																															
TIME																															

SECURITY CONTAINER CHECK SHEET

TO (if required)	**THRU** (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISOO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

DEPARTMENT OF HOMELAND SECURITY

CLASSIFIED DOCUMENT RECORD

Date

SECTION I. GENERAL

TO:	RETURN TO:

DATE RECEIVED	SUSPENSE DATE	REVIEW DATE	REGISTERED MAIL NO

CONTROL LOG OR FILE NO.	CLASSIFICATION	NUMBER OF COPIES	DESCRIPTION *(Unclassified Short Title)*	DATE OF DOCUMENT	ORIGINATOR

SECTION II. ROUTING

TO	COPY NO.	DATE	PRINTED NAME	SIGNATURE

SECTION III. DESTRUCTION CERTIFICATE (Check Appropriate Box)

MATERIAL DESCRIBED HERON HAS BEEN:

☐ **DESTROYED** ☐ **TORN IN HALF AND PLACED IN A CLASSIFIED WASTE CONTAINOR**

DATE	PRINTED NAME OF CERTIFYING/DESTR. OFF.	SIGNATURE

DATE	PRINTED NAME OF WITNESSING OFFICIAL	SIGNATURE

SECTION IV. REPRODUCTION AUTHORITY

NUMBER OF COPIES TO BE REPRODUCED	AUTHORIZED BY	DATE

SECTION V. RECEIPT/TRACER ACTION *(Check Appropriate Box)*

☐ **RECEIPT OF DOCUMET(S) ACKNOWLEDGED** ☐ **DOCUMENT(S) HAVE NOT BEEN RECEIVED**

☐ **TRACER ACTION: SEGNED RECEIPT FOR MATERIAL DESCRIBED ABOVE HAS NOT BEEN RECEIVED.**

DATE	PRINTED NAME AND TITLE	SIGNATURE

U.S. Department of Homeland Security

COURIER AUTHORIZATION REQUEST

REQUEST THE FOLLOWING NAMED INDIVIDUAL BE ISSUED COURIER AUTHORIZATION AS IDENTIFIED BELOW:

AUTHORIZATION TYPE (CHECK ONE): ☐ LAMINATED COURIER CARD ☐ ONE-TIME COURIER AUTHORIZATION		
NAME OF COURIER:	GRADE:	SOCIAL SECURITY NUMBER:
TITLE:	PHONE NUMBER:	
ASSIGNED ACTIVITY (INCLUDE MAILING ADDRESS):		
SECURITY CLEARANCE LEVEL (CHECK ONE): ☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐ SCI		
[1]HIGHEST CLASSIFICATOIN OF MATERIAL TO BE TRANSPORTED (CHECK ONE): ☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐ SCI		
AUTHORIZED GEOGRAPHIC AREA (E.G., NATIONAL CAPITAL REGION):		
DATE AUTHORIZATION REQUIRED (FOR ONE-TIME TRANSPORT ONLY):		
JUSTIFICATION:		
AUTHORIZING OFFICIAL (SUPERVISOR/MANAGER/COTR)		
NAME:	TITLE:	
SIGNATURE:		DATE:

COMPLETED BY SECURITY OFFICE
SECURITY CLEARANCE VERIFIED BY:

[1] The level requested for transport must be equal to or less than the security clearance level. The level requested for transport should reflect the actual need as opposed to the security clearance level. For example, because a person has a Top Secret security clearance does not mean they need to transport Top Secret materials – the need may be for only Secret. Therefore, the transport level requested should be Secret.

U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security
Office of Security

SECURITY PROCEDURES / ACKNOWLEDGEMENT FOR USE OF SECURE TELEPHONE UNIT-III (STU) * OR SECURE TERMINAL EQUIPMENT (STE) * IN AN OFFICE

The undersigned acknowledges, understands, and will comply with the following instructions governing the use of a STU/STE in an Office.

1. The STU/STE should only be used by the person for whom it is installed and will be strictly controlled while installed in my office. All of the security requirements will be observed for preventing unauthorized access to the keyed terminal and to classified and sensitive unclassified U.S. Government information.

2. I understand that the use of the STU/STE in the secure mode when discussing *classified* or *sensitive* information requires diligence. I will observe the display during initiation of a secure call to verify the identity of the remote party and to determine the highest classification level at which information may be discussed.

3. Only authorized persons will be allowed access to a keyed STU/STE.

4. To prevent unauthorized use and/or loss, the STU crypto ignition key (CIK) ***** or STE FORTEZZA® Plus (KOV-14) ***** Cryptocard will be removed when not in use. The CIK or KOV-14 will be in my personal possession or stored in a GSA approved security container when not in use.

5. I will not allow a foreign national to have access to the installed STU/STE in my office.

6. I understand that paragraph 1 states "the STU/STE should only be used by the person for whom it is installed." In addition, the STU/STE in some circumstances may be used on an occasional basis other employees in an office; however, such individual must not have access to the security-enabling component. Whenever possible uncleared employees should not have access to the STU/STE. Uncleared/unauthorized employees are restricted to only using the telephone in its commercial non-secure mode.

7. I will not use the STU/STE to discuss classified information when uncleared personnel are present.

8. The room in which the STU/STE is installed will have a lockable door which will be closed and locked during classified discussions.

9. I understand that if I take any classified notes, I will lock them in the GSA approved security container.

10. I will immediately report any unusual incidents concerning the location of the STU/STE, loss of CIK/KOV-14 or loss of STU/STE to the COMSEC Custodian who issued me the device.

11. I will ensure that both the STU/STE and CIK/KOV-14 are returned to the COMSEC Custodian when no longer required.

12. I understand that a hand receipt is used to record the acceptance of and responsibility for COMSEC material issued to a user by a COMSEC Custodian. **I also understand that as a hand receipt holder I must not allow the COMSEC equipment to be moved from its authorized location with out informing the COMSEC Custodian and that I am not authorized to reissue the material**. As a recipient I am relieved of responsibility for material received on a hand receipt when the material has been returned to the issuing COMSEC custodian and a copy of the voided hand receipt is given to me.

Print Name:_____

SSN: _____

Office Address:_____

_____

_____

_____

Work Phone: _____

STU/STE Secure Telephone No: _____

_____

Signature Date

***** Secure Telephone Unit III (STU-III) Type I is a dual-purpose telephone capable of transmitting voice and data. The STU-III Type I terminal may be used as an ordinary telephone with interoperability into the public telephone network. It may also be used as a secure telephone connectable through the public telephone networks to other STU-III Type I (classified/sensitive unclassified use) terminals. The STU-III terminal has a device called a crypto-ignition key (CIK) which locks and unlocks its secure mode.

Secure Terminal Equipment (STE) equipment is a flexible, adaptable telecommunications security solution for digital networks. Capabilities include removable FORTEZZA® Plus (KOV-14) Cryptocard, backwards compatibility with the STU-III, and software upgradeable. The telephone terminal must use a KOV-14 prior to transmission. The KOV-14 is used by the Government to protect classified information. The Cryptocard is the cryptographic enabling device for the STE.

STU-III/STE REKEY PROCEDURES

NSA requires all STU-IIIs and STEs be electronically rekeyed (replacement of operational key with new operational key by means of a telephone call to the **NSA Electronic Key Management System (EKMS) Central Facility** **at least once annually** to ensure the key remains current. DHS Office of Security guidelines stipulate that respective STU-III/STE **must be rekeyed semi-annually.**

Each STU-III user shall program the **EKMS Central Facility** telephone numbers ***(1-800-635-6301 or 410-526-3200, if you are in Maryland)*** in their Memory Dial Keys.

1. Remove your KSD-64A/Crypto Ignition Key (CIK) from your security container.
2. Insert the CIK into the STU-III KSD-64A Receptor on the side of the STU-III to make a secure call.
3. Call the EKMS Rekey Number – **1-800-635-6301**. Follow the recorded voice instructions for the rekey process. The STU-III will automatically "GO SECURE" and indicate a Rekey is in Progress. Observe the secure message window until it indicates the rekeying is complete.
4. Should rekey fail, use the following procedures:

   a. State and Local Users

   Contact the DHS Central Office of Record (COR) COMSEC Manager at (540) 542-5956 for technical support.

Note: If ***an emergency situation should arise and unable to contact the DHS COR COMSEC,*** State and Local Users can contact the DHS Office of Security COMSEC Manager.

b. DHS CSO Users: contact the CSO COMSEC Manager at (202) 692-4371 or (202) 401-4613 (STU-III) for technical support.

STE Rekey Procedures
(Programming the rekey numbers, if not already done)

1. Press **"Menu"** terminal displays "**Terminal Management**".
2. Press "**Scroll**" terminal displays "**Crypto Card Management**".
3. Press "**Select**" terminal displays "**Card Management Privileges**".
4. Select "**User"** terminal displays **"Rekey Functions".**
5. Press **"Select"** terminal displays **"Update Rekey Phone Number/Perform Rekey".**
6. Select **"Update"** terminal displays **"Update Stored Phone Number".**
7. Select **"STU-III".**
8. The **STU-III Rekey number** at **NSA EKMS 1-800-635-6301** should be stored in this field.
9. Repeat the above procedures for **"SDNS"** and ensure **1-800-633-3971** is stored for the FNBDT rekey.

STATE, LOCAL, AND PRIVATE SECTOR
STORAGE AND SAFEGUARDING STANDARDS FOR COLLATERAL CLASSIFIED INFORMATION

	[1]Federal Personnel Security Clearance	Analog Telephone Line	ISDN Telephone Line	[2]GSA Approved Storage Container	[3]Private Office	[4]Document Shredder	[5]Intrusion Detection Alarm System	[6]Federal Agency Approved Open Storage Area	[7]Standard Operating Procedures
Person to Person verbal-only access to classified information	X								
Secure Telephone (STU-III/STE)	X	X For STU-III Only	X For STE Only	X	X				
Secure Telephone (STU-III/STE) w/Secure Fax	X	X For STU-III Only	X For STE Only	X	X	X			
Secure Video Teleconference	X		X	X	X	X	X	X	X
Closed Storage of CONFIDENTIAL and/or SECRET Information	X			X	X	X			
Closed Storage of TOP SECRET Information	X			X	X	X	X		
Installation of Classified Computer System, e.g., HSDN	X			X	X	X	X	X	X

[1] Security Clearance must be granted by a Federal Executive Branch Agency and be equal to or higher than the level of classified information the person will access.

[2] Refer to enclosed product cut-sheet.

[3] STU-III/STE shall be installed in a private office or area having sufficient acoustical protection and physical controls to prevent conversation being overheard by unauthorized persons.

[4] For the destruction of classified information, document shredders must meet Federal standards for particle size. Contact the DHS Office of Security for approved shredders and vendors.

[5] Refer to DHS guidance on Open Storage Areas for information on Intrusion Detection Alarm Systems.

[6] Refer to DHS guidance on Open Storage Areas for information on structural requirements.

[7] Refer to DHS guidance on Open Storage Areas for information on Standard Operating Procedures.