Information Security Webinar Series

Storage of Classified Information

According to DoD Manual 5200.01, Volume 3, Enclosure 3, "Classified information shall be secured under conditions that are adequate to deter and detect access by unauthorized persons." In addition, classified holdings should not be stored with items such as weapons, funds, jewels, precious metals, or drugs. Classified holdings should be reduced to the minimum required to accomplish the mission.

> **"Classified information shall be secured under conditions that are adequate to deter and detect access by unauthorized persons."**

Storage Standards

The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for storing and protecting classified information. The Director of National Intelligence (DNI) establishes security requirements for Sensitive Compartmented Information Facilities (SCIFs).

Protection when Removed from Storage

Material removed from storage must be kept under constant surveillance. Document cover sheets assist in preventing inadvertent disclosure of classified information by someone who does not have a need-to-know.

SF 703 Top Secret Cover Sheet

SF 704 Secret Cover Sheet

SF 705 Confidential Cover Sheet

End of Day Security Checks

The heads of activities that process or store classified information are required to establish a system of security checks at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secure. The SF 701, which is the "Activity Security Checklist," is used to record these checks.

An integral part of the security check system is the securing of all vaults, secure rooms, and containers used for storing classified material. The SF 702, which is the "Security Container Check Sheet," is the form used to record those actions.

Additionally, the SFs 701 and 702 are retained and disposed of as required by Component records management schedules.

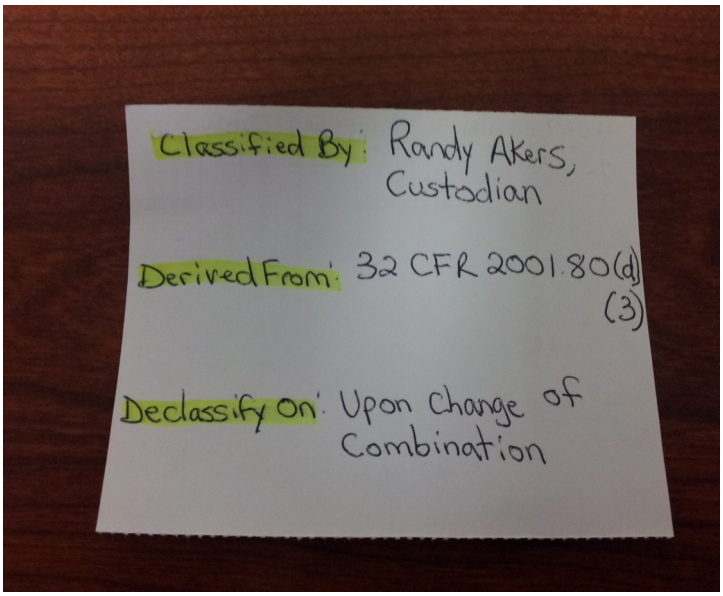
Security Container Information

The SF 700 is used to maintain a record for each container, vault, or secure room door used for storing classified information. The SF 700 is also updated every time the security container combination is changed.

The SF 700 is a two-part form. Part 1 is not classified, but it contains personally identifiable information (PII) that must be protected by sealing Part 1 in an opaque envelope. The envelope must be conspicuously marked "Security Container Information" and stored in accordance with SF 700 instructions. If the information must be

accessed during non-duty hours and a new opaque envelope is not available to replace the opened one, the original envelope can be temporarily resealed until Part 1 can be placed in a new envelope the next working day.

Part 2 of the SF 700 is classified at the highest level of classification authorized for storage in the security container. It must be sealed and stored in accordance with SF 700 instructions. The classification authority block shall state "Derived From: 32 CFR 2001.80(d)(3)" with declassification upon change of combination. The 32 CFR part 2001.80(d)(3) is the Information Security Oversight Office (ISOO) Classified National Security Information Final Rule for Executive Order 13526.



Working at Home

When mission critical for individuals to remove classified information and materials (e.g., IT equipment and associated storage media) for work at home, specific security measures and approvals are required. Security measures appropriate for the level of classification must be in place to provide adequate protection and security-in-depth and to prevent access by unauthorized persons.

Removal of Top Secret Information

Only the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, Combatant Commanders, or the appointed senior agency officials can authorize the removal of Top Secret information from designated working areas for work at home. Those same officials can also authorize removal of information for work at home for any lower level of classification, such as Secret or Confidential.

Removal of Secret and Confidential Information

Heads of the DoD Components can authorize removal of Secret and Confidential information from designated working areas for work at home. However, this authority will not be delegated below the major command or equivalent level.

Additionally, a GSA-approved security container will be furnished for residential storage of classified information, and written procedures must be developed to provide for appropriate protection of the information, including a record of the classified information that has been authorized for removal for work at home.

In the event classified IT systems and/or equipment will be used, reference Enclosure 7, Section 7 of Volume 3. Additionally, all residential classified network connections must be certified and accredited in accordance with DoD Instruction 8510.01, which is the DoD Information Assurance Certification and Accreditation Process (DIACAP).

Work at home may be authorized in foreign countries only when the residence is in a specific location where the United States enjoys extraterritorial status (e.g., on the embassy, chancery, or consulate compound) or on a U.S. military installation.

Lock Specifications

Combination locks on vault doors, secure rooms, and security containers protecting classified information must conform with Federal Specification FF-L-2740.

Classification Level Storage

Top Secret Information Storage

Top Secret information is stored:

In a GSA-approved security container with one of the following supplementary controls:

(a) either an employee cleared to at least the Secret level inspecting the security container once every 2 hours.

(b) or the location that houses the security container is protected by an intrusion detection system (IDS) meeting the requirements of Appendix 3 of the DoD Manual, with personnel responding to the alarm arriving within 15 minutes of the alarm's annunciation.

Top Secret information is also stored in a GSA-approved security container equipped with a lock meeting FF-L-2740 specifications, as long as the container is located within an area that has been determined to have security-in-depth.

Top Secret information is stored in an open storage area (also known as a secure room) constructed according to the requirements indicated in Appendix 3 and equipped with an IDS with personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth, or within 5 minutes of alarm annunciation if it has not.

Top Secret information is stored in a vault or GSA-approved modular vault meeting the requirements specified in Appendix 3.

Under field conditions during military operations, military commanders have the authority to judge the use of storage devices or security control measures adequate to prevent unauthorized access of Top Secret information. However, before they make their decision they should employ risk management methodologies to determine the appropriate safeguards.

Secret Information Storage

Any of the methods prescribed for Top Secret information storage may be used for Secret information storage. Secret information may be stored in a GSA-approved security container or vault built to the specifications indicated in Appendix 3 without the supplementary controls.

Secret information may be stored in an open storage area meeting the requirements outlined in Appendix 3, provided the senior agency official determines in writing that security-in-depth exists, and one of the following supplemental controls is utilized:

(a) either an employee cleared to at least the Secret level inspecting the open storage area once every 4 hours.

(b) or an IDS meeting the requirements outlined in Appendix 3 with the personnel responding to the alarm arriving within 30 minutes of the alarm's annunciation.

Secret information may be stored in a secure room that has been approved for the storage of Secret information by the DoD Component prior to October 1, 1995, provided the DoD Component reassesses the requirement for the secure room and makes plans to bring the room up to the standards indicated in the DoD Manual by October 1, 2013 and provided the area has been determined to have security-in-depth.

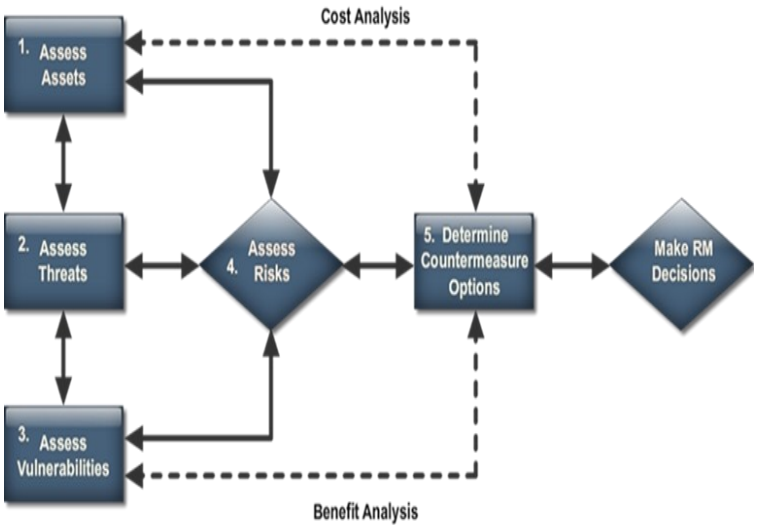
Confidential Information Storage

Confidential information is stored in the same manner as prescribed for Top Secret or Secret information excluding supplemental controls.

Risk Management

When considering the storage alternatives specified for storage of classified information by classification level, a risk assessment should be performed to facilitate a security-in-depth determination. This will also help identify and choose the appropriate supplemental controls that may need to be implemented. The analysis should, at a minimum, consider the local threats, both known and anticipated, and the vulnerabilities.

Additionally, the assessment should consider the existing security environment and controls and the ease of access to containers or other areas where classified data is stored. Moreover, the assessment should consider the criticality, sensitivity, and value of the information stored.



Lastly, incorporate an analysis of the cost versus benefits of potential countermeasures. Then use risk assessment to determine whether installation of an IDS is warranted and whether other supplemental controls are sufficient.

New Equipment Procurement

New security storage equipment is procured from those items listed on the GSA Federal Supply Schedule.

When GSA-approved security containers or vault doors with locks meeting FF-L-2740 are placed in service or when existing mechanical locks are replaced with locks meeting those same specifications, the custodian or security manager records the lock serial number on the SF 700.

If you have any questions about procurement or technical support, contact the DoD Lock Program at 1-800-290-7607 or DSN 551-1212.

External Markings

According to regulation, no external markings should be on the container revealing the level of classified information authorized to be or actually stored in the container or vault, or indicating the priority assigned to the container for emergency evacuation and destruction.

This doesn't prevent placing a mark or symbol (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes) or from applying decals or stickers that the DNI requires for containers and equipment used to store or process intelligence information.

However, in the event a GSA container or vault door recertification is required, those labels and markings must be removed, but they can be reapplied as needed after recertification.

Storage Area Entrances

When areas storing classified information are occupied by authorized individual(s), the entrances shall either be:

(1) Under visual control at all times to detect entry by unauthorized persons; or

(2) The entrance has to be equipped with an automated entry control system to limit access; see the Appendix to Enclosure 3 entitled Physical Security Standards.

b. Secure rooms or other areas storing classified information must be secured when the area is not occupied by authorized individual(s) or under continual visual control.

c. The Appendix to Enclosure 3 also provides standards for access control devices. Electrically actuated locks (e.g., magnetic strip card locks) do not, by themselves, meet the required standards for protecting classified information and cannot be used as a substitute for the locks prescribed in Enclosure 3, Section 2.

Foreign Government Information (FGI) Storage

To the extent practical, FGI should be stored separately from other information to facilitate its control. To avoid additional costs, separate storage may be accomplished by methods such as using separate drawers in the same container as other information or, for small amounts, the use of separate file folders in the same drawer.

How Can CDSE Help With Annual Briefings?

The Center for Development of Security Excellence (CDSE) produces and provides a wide range of information security training, education, and awareness products to support the DoD Activity Security Manager's mission.

This includes instructor-led training, eLearning courseware, and training products to address the entire range of responsibilities assigned to an activity security manager.

On the CDSE website you can find additional information about CDSE products, access eLearning courseware, register for instructor-led training, and download job aids and security awareness materials.

Learn more @ dssa.dss.mil

STEPP Learning Management System

A wide array of information security-related eLearning can be accessed on CDSE's learning management system called STEPP.

The STEPP system not only provides multimedia-rich courseware but also retains and maintains learner records and transcripts. STEPP is available for use by DoD and other U.S. Government personnel and contractors within the National Industrial Security Program.

Job Aids and Awareness Media

CDSE also produces various job aids to assist security professionals. They can be accessed on the CDSE website.

Job aid topics include Marking Classified Information, Derivative Classification Training, a Procedural Guide for Conducting Classified Conferences, and aids for the operation of standard locks.

Job Aids
www.dss.mil/seta/resources/supplemental-job-aids.html
Awareness Posters
www.dss.mil/seta/security_posters.html

Instructor-Led Training

DoD Security Specialist
Broad survey course that includes general, industrial, personnel, information, and physical security related-topics targeted to personnel with little or no security-related experience.

www.dss.mil/cdse/catalog/classroom/GS101.html

Information Security Management
Mid-level course intended for personnel who have a functional working knowledge of the DoD Information Security Program.

www.dss.mil/cdse/catalog/classroom/IF201.htm

Instructional Media

In addition to instructor-led and eLearning courses, CDSE also offers a wide variety of other instructional media in support of the DoD Information Security Program. This includes Security Shorts, which are targeted eLearning courses designed to be completed in less than 15 minutes. Other instructional media includes podcasts, which are audio-only based courses, and short training videos on various security processes and procedures.

Security Shorts
www.dss.mil/cdse/shorts
Security Podcasts
www.dss.mil/cdse/catalog/podcasts
Security Training Videos
www.dss.mil/seta/training_videos.html

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.