

LESSON TOPIC 5.6**Storage****REFERENCES**

SECNAV M-5510.36, Chapter 10

OPNAVINST 5530.14E, Physical Security and Loss Prevention

LESSON**A. Basic Policy for Storage (ISP 10-1)**

1. Commanding Officers shall ensure that all classified information is stored in a manner that will deter or detect unauthorized access when it is not under personal observation of cleared persons. Where possible limit storage for better control, protection and more efficient management
2. Report equipment weaknesses, deficiencies, or vulnerabilities to (CNO (N3AT) via DUSN(PPO&I)
3. Do not store weapons or pilferable items (e.g., money, jewels, precious metals or narcotics) in a security container used to store classified information
4. DO NOT place number/symbol on exterior of container to indicate priority in the event of emergency destruction (never show level of classified information stored)
5. Shipboard containers shall conform to DON standards for durability, size, weight, maintainability and safety. If existing Group 1R combination locks need replacement replace with combination locks meeting Federal Specification FF-L-2740 (X-07, X-08, or X-09)(**ISP 10-6**)

(Note supplement security measures will be implemented when surrounding area not manned by U.S. personnel)
6. Under field conditions during military operations, the Commanding Officer may require or impose security measures deemed adequate to meet the storage requirements

B. Storage Requirements (ISP 10-3)

1. If classified information is not under the personal control/observation of a cleared person - it shall be guarded or stored in a:
 - Locked GSA-approved security container
 - Vault,
 - Modular vault, or
 - Secure room (open storage area constructed per Exhibit 10A ISP) (see NTD 03-09 for a checklist to assist with validating the requirements for a Secure Room)

2. Top Secret - Store by one of the following methods:
 - a. In a GSA-approved security container with one of the following supplemental controls:
 - Location housing the security container is subject to continuous protection by cleared guard or duty personnel;
 - Cleared guard or duty personnel shall inspect security container once every 2 hours;
 - An IDS with personnel responding to the alarm within 15 minutes of the alarm annunciation; or
 - Security-in-Depth (e.g., guard, watch, access control) when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740 (X-07, 8, 9 locks)

 - b. In a vault, modular vault or secure room constructed per exhibit 10A, equipped with an IDS and a personnel response to the alarm within: (1) 15 minutes of the alarm annunciation if the area is covered by Security-in-Depth, or (2) 5 minutes alarm response if it is not covered by Security-In-Depth

(Open storage areas constructed per exhibit 10A shall be designated in writing by the Security Manager **CNO ltr 5510 ser N09N2/9U223112 of 7 May 09, Interim Policy Changes, Reminders and Clarifying Guidance to SECNAV M-5510.36**)

3. Secret - Store by one of the following methods: (1) In the same manner prescribed for Top Secret; or (2) In a GSA-approved security container, modular vault, or vault without supplemental controls. In a secure room use one of these supplemental controls:
 - Continuous protection by cleared guard or duty personnel (or)
 - Inspected every four hours
 - IDS with 30 minute response (changed from 15)
4. Confidential - Store in the same manner prescribed for Top Secret or Secret except that supplemental controls are not required
5. Storage areas for bulky Secret and Confidential information. Secure access openings with GSA-approved combination padlocks (Federal Specification (FF-P-2890 series) or high security key-operated padlocks or Federal Specification (MIL-P-43607). (Combination padlocks are removable from container) Area in which container is stored shall be locked when not manned by U.S. personnel and checked once every 24 hours

C. Procurement of Security Containers (ISP 10-4)

1. First, ensure need: Survey equipment, review volume of records, and determine records cannot be reduced to fit existing space
2. Check with DRMO) for usable containers prior to purchasing new ones

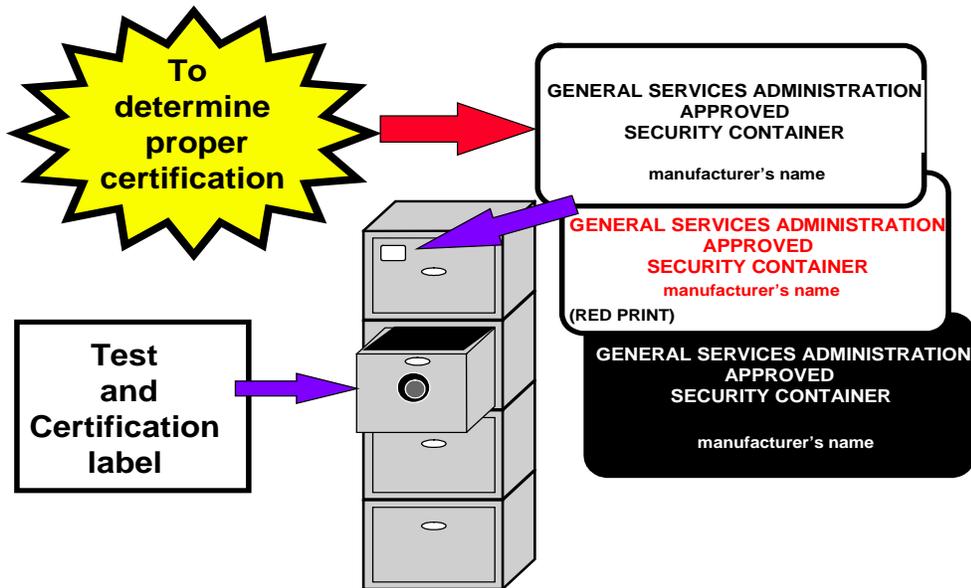


Figure 5.6-1. Security Container Certification.

1. To determine proper certification, look for: (see figure 5.6.1)
 - a. GSA Approval Label on the outside of the top drawer (usually on left) of containers produced after 1962
 - Containers manufactured before Oct 1990 the GSA approved label will have either black lettering on a silver background or silver on black
 - Containers manufactured after Oct 1990 have a silver label with red lettering or red with silver lettering
 - Information Processing System (IPS) containers for IT systems have blue lettering labels
 - b. GSA Test and Certification label located on the inside of the locking drawer wall

(If container or vault door does not have the GSA Approved label - it must be inspected and recertified by trained personnel before it can be used to store classified information)
4. Purchase only GSA approved containers. At present, only classes 5 and 6 are available on GSA schedule but properly certified classes 1 through 4, 7 & 8 may still

be used to store classified information

5. GSA-approved field safes and special purpose one and two drawer, light-weight security containers

- Intended primarily for storage of classified information in situations where normal storage not feasible

- Must be securely fastened to structure to render them non-portable or kept under constant surveillance

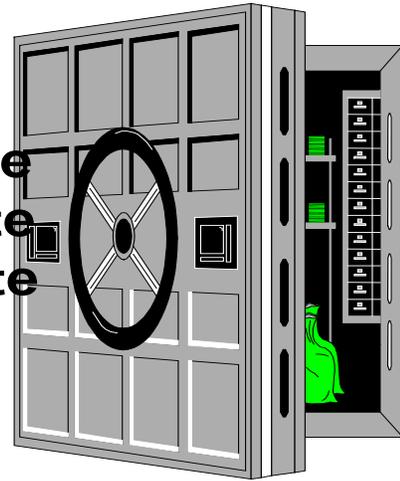
D. Vaults and Secure Rooms (ISP 10-7) (see figures 5.6-2 and 5.6-3)

1. Often used to meet open storage requirements for large amounts of classified information, or for odd-shaped or bulky material
2. Construction
 - a. Must be built to standards specified in SECNAV 5510.36, Exhibit 10A
 - b. The Military Handbook 1013/1A "Design Guidelines for Physical Security of Facilities" June 28, 1993 provides detailed construction criteria for vaults and secure rooms and is normally held at Public Works
 - c. Secure rooms can minimize need for GSA-approved security containers (**ISP Exhibit 10A**)
 - d. Periodically examine existing vaults and secure rooms; make repairs promptly
 - e. GSA approved modular vaults meeting Fed Spec AA-V-2737 may be used to store classified information
 - f. Entrances to vaults or secure rooms shall be under visual control at all times when occupied to prevent entry by unauthorized personnel or equipped with electric mechanical or electro-mechanical access control devices to limit access

Vaults

The Military Handbook 1013/1A Design Guidelines for Physical Security of Facilities

- ▣ **Floor - 8 inches concrete**
- ▣ **Roof - 8 inches concrete**
- ▣ **Walls - 8 inches concrete**
- ▣ **Door - Class 5**



NOTE: All concrete must be **reinforced**

Figure 5.6-2. Vaults

Secure Room

IDS
Requirements

Walls
Floors
Roof
Ceiling



Permanent Construction Materials; i.e. plaster, gypsum wallboard, metal panels, hardboard, wood, etc.

Doors



**Wood or Metal
Combination Lock
Dead bolts**

Windows

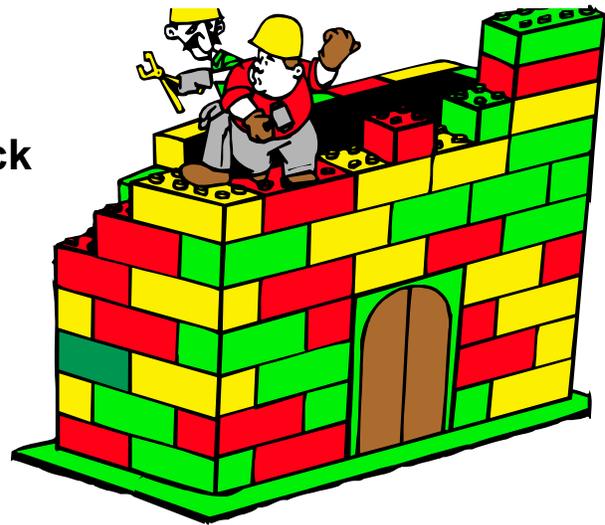


**Same Strength
as contiguous
walls**

Other
Openings



96 Sq inches



NOTE: Combination Locks must meet Fed Spec FF-L-2740

Figure 5.6-3. Secure rooms.

E. Requirements for Residential Storage (ISP 10-10) CNO ltr 5510 ser N09N2/9U223112 of 7 May 09, Interim Policy Changes, Reminders and Clarifying Guidance to SECNAV M-5510.36 (see figure 5.6-4)

1. Critical operational requirement must exist
2. Commands shall develop written procedures to clearly delineate the following:
 - Classified information must be under personnel control of the authorized individual when not secured in a GSA-approved security container
 - Identification and signature receipt and

reconciliation upon return of the classified information

- Information shall be stored in a GSA-approved container protected with IDS or equivalent supplemental controls

- Furnish a copy of all residential storage approvals to DUSN(PPO&I)

Residential Storage Approval Authorities	Top Secret	Secret/Confidential
SECDEF	X	X
SECNAV	X	X
COMBATANT COMMANDERS	X	X
CNO (N09N)	X	X
CMC		X
FLEET COMMANDERS*		X
COMMANDER NAVAL SPACE CMD		X
COMMANDERS NAVSYSCOMS		X
CHIEF NAVAL RESEARCH		X
CG MARFORLANT/PAC		X
CG COMBAT DEVELOPMENT CMD		X
CG MARINE CORPS SYSTEM CMD		X

*CFFC, PACFLT, NAVEUR and NAVCENT

Figure 5.6-4. Residential Storage Approval Authority

F. Combination Locks (ISP 10-11)

1. GSA certified electromechanical combination lock meeting Federal specifications FF-L-2740 (X-07, X-08, or X-09)

- Installed on all new GSA containers since October 1991, and shall be used when replacement locks are needed. Existing mechanical locks may not be repaired; must be replaced with FF-L-2740 locks

- Commands must have a plan for replacement of mechanical locks protecting classified information with FF-L-2740 locks (See ISP Exhibit 10B)

2. To ensure combination locks are effective: **(ISP 10-12)**

- a. Combination changes can be made only by individuals with that responsibility and appropriate security clearance level
- b. Give combinations only to those whose official duties require access and change combinations when:
 - Containers or locks are first placed in use
 - An individual who knows combination no longer requires access **unless** sufficient controls exist to prevent access to the lock
 - Combination was subjected to possible compromise
 - Taken out of service. (Reset: Built-in combinations to 50-25-50, and Padlock combinations to 10-20-30)
- c. In selecting combination numbers do not use sequential numbers, simple ascending or descending number series or personal data and do not use the same combination for more than one container

(After changing a combination and to prevent a lockout - before closing container or vault, it is good practice to have two people try the new combination three times with locking drawer/door open)

**G. Standard Form 700 (Security Container Information)
(ISP 10-12)**

1. Maintain a SF 700 (use current form dated April 2001) for each vault, secure room, or container used to store classified information. Follow instructions on the form
2. Mark Parts 2 and 2A with the security classification of the highest category of material authorized for storage in the vault, container, or secure room; safeguard and store the SF 700 based on its security classification
3. Place Part 1 in interior location of container, vault or secure room with names, home addresses, and home phone numbers of individuals to be contacted in the event the security container, vault or secure room is found open and unattended

4. Mark Parts 2 and 2A with highest classification level of information stored therein and place in another container, vault or secure room as appropriate for classification

H. Key and Padlock Control

1. Commanding Officers - Establish administrative procedures for control and accountability of keys and locks whenever high security key-operated padlocks are used
2. Level of protection provided each key will be equivalent to highest classification level of information being protected by padlock
3. TITLE 18, U.S.C., SECTION 1386 makes unauthorized possession of keys, key blanks, keyways, or locks used in the protection of classified information a criminal offense
4. OPNAVINST 5530.14E governs keys and locks used for protection of classified information

I. Repair and Maintenance of security containers (ISP 10-15)

1. Neutralization of lock-outs, repairs and maintenance of GSA-approved security containers shall be per "Federal Standard 809" and done only by authorized individuals who have a favorable trustworthiness determination or are continuously escorted (see ISP 10-15 for details on lock-outs, repairs and maintenance)
2. Enter maintenance, repairs or damage, and periodic inspections on the Maintenance Record for Security Containers & Vault Doors, GSA Optional Form 89 (See ISP Exhibit 10C for Optional Form 89)
3. External modification of GSA-approved security containers to attach additional locking devices or alarms is PROHIBITED

K. Electronic Security System (ESS) (ISP 10-16 and Exhibit 10D)

1. An ESS consists of one or a combination of:
 - Intrusion Detection System (IDS)

- Closed Circuit Television (CCTV)
 - Access Control System (ACS)
2. IDS provide a means to detect and announce proximity or intrusion - NOT prevent. They are used to:
 - Permit more economical/efficient use of manpower
 - Take the place of other elements of physical security which cannot be used
 - Provide additional controls to vital areas
 3. Four distinct phases of operation of ESS components are:
 - Detection
 - Reporting
 - Assessment
 - Response
 4. Testing of both ESS equipment and guard response time is essential in establishing and maintaining system reliability.
 5. Descriptions and examples of IDS and ACS can be found in Exhibit 10D, ISP