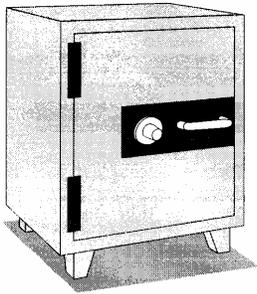


LESSON 7

SAFEKEEPING AND STORAGE



Since most classified information spends far more time not being used than being used, the safekeeping and storage of classified information is extremely important. And sometimes the measures that the Government takes to safeguard classified information are surprising. Did you know, for instance, that of the two approved stand alone containers for Secret information, one provides little protection against forced entry - and the other provides none at all? In this lesson, we'll explore the rationale behind this apparent lack of security: the concept of risk management. We'll also explore the literal "nuts and bolts" of security - the physical equipment and devices used to store classified information. We'll see when to use them, how to procure them, and how to keep track of the level of classified in each of them. We'll talk about the locks and locking devices that secure them and how to handle the combinations for them. We'll wind up with a few words on repairing them and on safeguarding classified information in foreign countries. At the end of this lesson, you will be able to do the following:

- Identify the types of threats that security containers and facilities for classified storage are designed to protect against.
- State the principle of risk management.



Lt. Col. Bill Timmons

- Identify storage requirements for the different levels of classified information.
- Select the locks used for protecting bulky classified materials and state the procedures used with the locks.
- Select and procure appropriate storage equipment for classified information.
- State the procedures for designating containers.
- List the conditions that require changing a combination.
- Identify properly restored security equipment.
- List the methods of safeguarding classified information in foreign countries.

Storage equipment and procedures seldom change, so people tend to take them for granted and often become careless about their use. This is no less a problem for DIVA than for any other organization or agency.

To reduce the danger of such carelessness, Lt. Col. Bill Timmons, Chief of the Security Branch, routinely assigns a new person to the job of overseeing the procedures for use and security of storage containers within DIVA. Mike Carson, a new hire, was recently appointed to replace Wally Chin for these duties.

Let's look in on their meeting in Wally's office.

Types of Threats

"Mike," Wally says, "the first thing to keep in mind is that we try to provide protection against two types of threats.

We try to protect against...

- **Inadvertent disclosure**
- **Deliberate attempts to gain access**

Mike knew that inadvertent disclosure was when classified information is disclosed *unintentionally*. "It seems to me," says Mike, "that inadvertent disclosure would most likely occur when classified documents or materials are in use. Isn't that why we use cover sheets? So that no unauthorized person - even someone who doesn't mean to - can look down at an open document on a desk and see classified information not intended for his eyes?"

"That's true," says Wally. "Inadvertent disclosure can even occur while a person is removing a classified document from a storage container or replacing it. But imagine how much inadvertent disclosure there would be if classified information were stored in unlocked, easily accessible containers! Unauthorized persons could accidentally open a file with classified while innocently searching for unclassified materials. Secure containers prevent this threat."

"I can see that," Mike says, "But what about *deliberate* attempts to gain access? Why doesn't everyone use the best safe available?"

"Actual dollar *costs* limit the practicality of that approach," says Wally. "Besides, *no container exists that can defend against a determined effort to gain access.*"



"Faced with these real world considerations, the *Government does not seek absolute physical security of all classified information.* Instead, the Government relies on the fact that a person who wants to gain illegal access to classified information *does not want to leave evidence* that the information has been compromised. For one thing, discovery of the compromise would bring on an investigation and the possibility of apprehension. Then, too, when the Government detects a compromise, the information usually loses its value, since the Government can take action to counteract the damage. And so we focus on *deterrence through probable detection.* For one thing, we use safeguards that would show, *by the evidence left,* that a breach in security has occurred.

Risk Management

"At the same time, though, we don't want to make it easy to get at classified information! If all we cared about were the evidence left, we could just blow up a balloon around the information every night when we left! What we want is protection that *makes a forced attempt to gain unauthorized access obvious* and that *substantially prolongs a more subtle attempt,* such as manipulating the combination dial.

With enough delay, the attempt will be thwarted by the arrival of installation personnel.

"Since we are *not* seeking *absolute security*, we are willing to take certain risks. Security of classified information may be compared to the safety of the car that you drive. Most of us do not select the absolute 'safest' car on the road. We compromise. Big cars are usually safer than small ones, but most of us don't buy the biggest car because of parking, maneuverability, and cost.

"Within the constraints of our needs, desires, and funds, we set an *acceptable level of risk* or *minimum risk* that we will have an accident or be injured in an accident.

The same is true for security of classified information. Our main goal," Wally continues, "is to provide a minimum risk that deliberate attempts to gain access will be successful.

"We base the *level of the risk* on the *level of classification* of the information that we are protecting. The *higher* the classification of the material, the *lower* the risk we are willing to take. And so the *higher* the classification, the *more stringent* is the physical protection standard for that material."

RISK MANAGEMENT

- * **Based on level of classification**
- * **Local situations can influence how much risk is taken**

"Does that mean that the same information may be protected in different ways at two different locations?" asks Mike.

"That's exactly right," says Wally.

Storage methods vary according to the *nature and size of the activity* its *mission* and the *level and type of classified information*.

"The effectiveness of the storage methods may be equal even though the methods themselves are different."

"I'm not sure what you mean by that," Mike replies.



"Well, for example, at one installation they may be storing Confidential documents in a GSA-approved security container that is located in a locked office with no alarms or any other security measures to protect the container. At another installation, the same document might be openly stored in a locked secure room that is protected with an alarm system as well as a magnetic badge reader. Both systems do the job."

"And notice that they both use *several* security measures. You should not use just a security container by itself when securing classified materials. Storage procedures should incorporate other physical security elements, such as locked doors, location of containers, and container records."

Mike says, "Still, there are times when a container can be used by itself, right? So doesn't there have to be some uniformity in the protection they provide? Don't they have to meet some sort of standards?"

Standards for Storage Equipment

"You bet they do, Mike."

There is a security container in the office and Wally walks over to it.

"This cabinet had to meet the *General Services Administration's* (GSA) criteria for storage equipment used for classified information."

The GSA establishes and publishes minimum standards, specifications, and supply schedules for:

- **Containers**
- **Vault doors**
- **Modular Vaults**
- **Alarm systems**

and

- **Associated security devices suitable for the storage and protection of classified information.**

"GSA writes the specifications for the containers, then the container manufacturers submit their products for testing against the standards. If the product meets the specifications, GSA certifies it. GSA does the same for vault doors and for modular vaults.

"Alarm systems and associated security devices that are used to protect classified information should also meet standards set by GSA. Associated security devices are biometric machines used to determine if a person is authorized access to the classified materials - fingerprint readers, palm geometry readers, retinal eye scanners, etc. GSA is currently updating these specifications. When they are finalized, GSA plans to implement testing and certification procedures.

"And take a look at this," Wally says, pointing to the label affixed to the *outside of the locking drawer*.



General Services Administration
Approved Security Container

"When you see this GSA *approval* label you know that the cabinet was manufactured *after 1962*. That's when GSA formalized the certification program and started placing this label on storage equipment authorized for classified materials."

Mike sees a second label located on the *side of the container's locking drawer*. "What's this, Wally?"

THIS IS A U.S. GOVERNMENT CLASS 6 CABINET WHICH HAS BEEN APPROVED BY GSA UNDER FEDERAL SPECIFICATION AA-F-358G. IT AFFORDS THE FOLLOWING PROTECTION:

- 20 MAN-HOURS AGAINST SURREPTITIOUS ENTRY
- 30 MAN-MINUTES AGAINST COVERT ENTRY
- 0 MAN-MINUTES AGAINST FORCED ENTRY

"It's a GSA *test certification* label, Mike. With older equipment you sometimes find it on the inside wall. Notice that the label shows *zero man-minutes against forced entry*. Remember what I said earlier about deterrence through probable detection? When individuals (or governments) want illegal access to classified information, they usually want that access to occur in such a way that the authorized holder of the information does not know that the information was compromised. We say they want the entry to be *covert* or *surreptitious*, an entry that does not leave physical evidence. So even though the cabinet itself can be broken into in nothing flat, it is a rare situation when someone uses a sledge hammer to open it to get at classified materials!

"And here's the *identification* label," Wally says. "It contains four items of information.

- 1. Cabinet Model**
- 2. Serial Number**
- 3. Year of Manufacture**
- 4. Contract Number**

"It's important to know that this information can be found on this third label," says Wally, "because every once in a while we receive notices about taking certain actions with containers. And the criteria that the notices use to identify the affected containers are the data on this label."

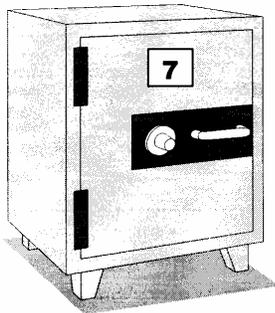
"Is there a way for a visitor to know the classification of material stored in any container simply by looking at it?" Mike asks.

"No," says Wally. "For one thing, it's acceptable to store Secret and Confidential documents in Top Secret storage devices. So it's conceivable that a container in which it's O.K. to store Top Secret materials might only contain a Confidential document. Then, too, heads of DoD Components may establish more stringent standards. Thus standards may vary among components. If that weren't enough, it is also *prohibited* to indicate the authorized level of storage on the outside of a container!"

Storage Requirements for Classified Information

"I haven't thought a lot about the container that I use to store my Secret documents," says Mike. "I guess I just assume that it meets the standards for Secret storage."

"Can you describe the container and its locking mechanism?" asks Wally.



"It's the gray safe in my office. It has a sticker with the number 7 on the outside. It has a 3-position combination lock. I'm pretty sure that there's a test certification label inside."

"Good old number 7!" says Wally. "It meets the container standards for storage of Top Secret information."

"I know it's been some time since you studied the minimum requirements for storing classified materials. Let me review them with you."



Top Secret information can be stored in a...

- GSA-approved security container with supplemental controls
- Vault (meeting DoD standards) with IDS
- GSA-approved modular vault with IDS
- Secure room (meeting DoD standards) with IDS

"IDS stands for *intrusion detection system*. An IDS is an electronic alarm system that operates by detecting motion, heat, sound, or other disturbance in the protected area. Note that if you store Top Secret materials in a GSA-approved security container, *supplemental controls* must be applied.

Supplemental Controls for
GSA-Approved Security Container
Storing Top Secret Information

One of the following must be applied *in addition to the container itself*.

1. A location under continuous protection by cleared guards or duty personnel
2. Inspection of the container once every 2 hours by cleared guards or duty personnel
3. An IDS which meets the standards specified in DoD 5200.1-R
4. Security-in-depth if the container has the Kaba-Mas (formerly Mas-Hamilton) X-07, X-08, or X-09 locks

"You can also use a vault, a GSA-approved modular vault, or a secure room to store Top Secret material.

Top Secret Storage – Compartments

A vault must meet the specifications noted in DoD 5200.1 -R *and be* protected by IDS or be under constant surveillance.

A GSA-approved modular vault must be protected by IDS or be under constant surveillance.

A secure room must meet the specifications noted in DoD 5200. 1-R *and be* protected by IDS or be under constant surveillance.

Mike asks, "What about Secret information? Does it have to be stored exactly like Top Secret?"

"The requirements are not as stringent," Wally replies. "Secret information is not as sensitive as Top Secret information, so we are willing to take a little more risk with it."

Secret information can be stored in...

- The same manner prescribed for Top Secret storage
- GSA approved security container or vault without supplemental controls
- A secure room (meeting standards established prior to 1 Oct 95 by the head of the DoD Component concerned)

"Confidential materials can be stored in the same containers or facilities as Secret materials and do not require supplemental controls."

Minimum Storage Requirements

Top Secret	Secret	Confidential
<ul style="list-style-type: none"> • GSA approved container with supplemental controls • Vault with IDS • GSA approved modular vault with IDS • Secure room with IDS 	<ul style="list-style-type: none"> • Same as TS • GSA approved container or vault without supplemental controls • Secure room approved by Component Head prior to Oct 95 	<ul style="list-style-type: none"> • Same as Secret without supplemental controls

Storing Bulky Materials

"What about storing bulky classified items, like equipment?" Mike asks. "I know we don't have any here at DIVA, but how is it stored?"

"Good question," Wally replies. "Bulky materials, other than those classified Top Secret are stored in areas that can be secured with special padlocks."

Storage of Secret and Confidential Bulky Material

Bulky materials will be stored in areas that have access opening secured by GSA-approved padlocks.

"The *combination padlocks* must be of the Federal Specification FF-P110 series. The padlock that currently meets the specification is the *Sargent & Greenleaf model 8077AC*. If you use a *key-operated padlock*, it must be a shrouded shackle padlock, which meets Military Specification P-43607. The key-operated padlock that currently meets the specification is the *Sargent & Greenleaf model 833*.

"And if a *key-operated padlock* is used, the keys must be *treated as classified material equal to the classification of the material being protected*. And administrative procedures for the control and accounting of the keys and locks must be established, such as appointing a key control custodian, regular inventorying of keys and locks, regular rotation of locks, and signing for keys. The 5200.1-R does not specify all of the administrative

procedures, but the procedures for any good key control system would be applicable."

Procurement of New Storage Equipment

"Suppose I need a new security container," Mike says. "Where do I look to find out what's available?"

Wally answers, "If you are going to purchase a new security container, you need to use the GSA Federal Supply Schedule.

Procurement of New Storage Equipment

New security storage equipment must be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by heads of DoD Components, with notification to USD(I).

"The *Federal Supply Schedule (FSS) for Miscellaneous Furniture* lists the different types of containers and the various configurations (each designed for a different purpose). Read the descriptions carefully. It is easy to make a mistake and order the wrong type of container. The FSS also provides instructions for ordering."

Designations and Combinations

As Mike and Wally continue their rounds they come upon an office with the remnants of a small party that had been held earlier in the day. Wally tells

Mike, "This is a good time to explain about *designations* and *combinations*.

"Make a note about that container in the corner, the one with the red number on the side. One of your first duties after this briefing can be to see that the combination on the lock is changed.

"You're already aware that there can be no external indication of the classification level of materials stored in a container. However, containers can be *identified* to tell them apart. Each container may be labeled on the outside with a *number* or *symbol*. At DIVA we use numbers.

For identification purposes...

Each vault or container may be given an external number or symbol.

"Each container has been assigned a level of classification to be stored in it. Only information of the assigned and lower levels may be stored in it. As you carry out your new duties you will become familiar with the designation of each classified material storage container within DIVA.

"One reason that you need to know about each container is so that you can ensure that the combination is changed at the right times. One of your responsibilities is to help people change combinations of locks when necessary. For example, until noon today, Frank Lewis was authorized access to the classified information in container '4.' However, he was transferred to another job - hence the party - and no longer requires that access.

"An important part of your job will be to maintain the records of the *combination of the lock, the location of the container, and the names, addresses and telephone numbers of the people who know the combination.*"

Once the combination has been changed and made known to authorized individuals, record the information on a *Standard Form 700, Container Information*. Remember that the combination has the *same security classification* as the information in the container. Thus any *record of the combination* must be stored in a *container approved to store material with that level of classification* or a higher level."

"I can see why combinations should be changed when persons are reassigned and no longer require access to the materials," says Mike. "What other events require combination changes?"

"Several conditions require changing combinations.

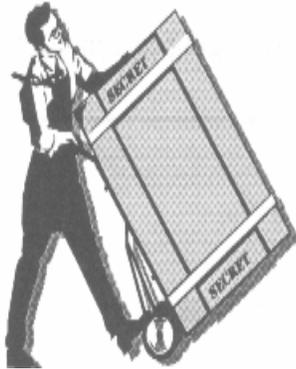
Combinations shall be changed...

- When the container or padlock is first placed *in use*.
- Whenever an individual knowing the combination *no longer* requires access or is no longer authorized access unless other sufficient controls exists to prevent access to the lock.
- When the combination has been subject to possible compromise.
- When the container or padlock is taken out of service.

"When a container is first brought into an office, the combination on the lock will be 50-25-50. Be sure that you remind people that '50-25-50' is *a standard*

setting and that they have to put on their own unique combination right away. And Mike, remember when we talked about using a combination padlock for the storage of bulky items? All of the procedures I just mentioned concerning changing combinations apply to those padlocks also. (The standard setting for the padlock is '10-20-30.')

Repair of Damaged Security Containers



"Mike, your new responsibility also involves attention to *repair of damaged equipment*. When containers or locks are damaged it can often be more economical to repair the damage or replace damaged parts rather than replace the whole piece of equipment."

"I've never seen any damaged equipment before. What type of damage occurs?" asks Mike.

"Equipment does not fail often," replies Wally. "However, the most usual problem is a *lock failing to operate properly*."

"Replacement of damaged or altered parts is fairly cut and dried. For example, a damaged lock can be replaced with a currently authorized lock. The equipment is then considered restored to its original state of security."

.... Repairing security containers is not so simple. The repair standards can be found in DoD 5200.1-R. If you wish to continue to use a damaged container as a GSA-approved one, you must ensure that the container is repaired in the specified manner. In making repairs to security containers, the following general rules apply.

Repair of Damaged Security Containers

- Only *authorized persons*, cleared or continuously escorted, may make repairs.
- To be considered repaired, strict *standards must* be met.
- If repair standards are not met, the Test Certification *Label and the GSA approval label must be removed*.
- A container not meeting repair standards may be used only for *unclassified* materials and must be so *marked on* the front.

Safeguarding Classified in Foreign Countries

Mike does not have to *safeguard classified information in foreign countries*. However, you may be called upon to do just that. Be aware that U.S. classified materials should be retained in foreign countries only when *absolutely necessary*.

Classified material in a foreign country that is not authorized for release to that country may be stored...

- At a U.S. military installation, embassy, or consulate
- At a building used exclusively by U.S. government tenants if the building is under 24-hour control by U.S. government personnel
- At a building not used exclusively by U.S. Government tenants if the information is stored in GSA-approved containers and
 - a. under 24-hour U.S. control by a U.S. Government activity (when the host government does not control the building)
 - b. in a locked room or area to which only U.S. personnel have access (when the host government controls the building)

Control procedures for information that has been authorized for release will be specified in the appropriate agreement.

Summary



We have discussed safekeeping and storage of classified information. Containers and storage facilities provide protection against inadvertent disclosure and deliberate attempts to gain access. Since there is no entirely secure container and since costs to provide the best security container across the board are too high, we do not seek absolute security. Instead, we rely on deterrence through probable detection, knowing that those who are most likely to try to gain unauthorized access to classified material want to avoid discovery. We seek risk management, and set a level of protection appropriate for each level of classification. The specific conditions at an activity also affect the amount of risk taken. The General Services Administration (GSA) sets the security standards for containers, vault doors, modular vaults, alarm systems, and associated security devices. GSA approved containers bear an approval label, test certification label, and identification label. Top Secret information may be stored only in a GSA approved security container with supplemental controls, a vault or secure room that meets DoD standards and has an intrusion detection system (IDS), or a GSA-approved modular vault with IDS. Secret material may be stored in the same manner as Top Secret information, in a GSA-approved container or vault without supplemental controls, and in a secure room that meets appropriate standards



Confidential information may be stored in the same containers or facilities as Secret information but does not require supplemental controls. Bulky materials are stored in areas secured with either the Sargent & Greenleaf 8077AC combination padlock or the Sargent & Greenleaf 833 key-operated padlock. New security containers are procured using the Federal Supply Schedule for Miscellaneous Furniture. Security containers may not be marked to show the level of classification they contain, but may be identified by a number or symbol. A combination used in securing classified material has the same classification as the most sensitive information it protects, and any record of the combination must be stored according to that classification. Combinations must be changed when the container or padlock is first placed in use, whenever an individual knowing the combination no longer requires access or is no longer authorized access, when the combination has been subject to possible compromise, and when the container or padlock is taken out of service. Only authorized persons may repair damaged containers and if strict standards are not met, the GSA approval and test certification labels must be removed and the container used to store unclassified materials only and so marked. Classified information in a foreign country may be stored at a U.S. military installation, embassy, or consulate; at a building used only by U.S. government tenants if it is constantly controlled by U.S. personnel; or at a building used by non-U.S. tenants if the information is stored in GSA approved containers and either under 24-hour control by a U.S. activity (if the host government does not control the building), or in a locked room or area to which only U.S. personnel have access (if the host government controls the building).

REVIEW EXERCISES

1. The Information Security Program seeks to provide protection against what two threats?
 - a. _____
 - b. _____

2. Risk management acknowledges that it is practically impossible to provide security against all attempts to gain illegal access to classified information. Instead, we try to keep the risk of illegal access to a minimum. We base the level of risk that we are willing to take on the _____ of the information we are trying to protect. In addition, _____ can influence how much risk is taken.

3. The storage methods for classified information vary among activities. List three factors that influence the methods of storage.
 - a. _____
 - b. _____
 - c. _____

4. Name the five types of equipment for which the General Services Administration publishes minimum standards.
 - a. _____
 - b. _____
 - c. _____
 - d. _____
 - e. _____

5. The three labels that can be found on a GSA-approved security container are the GSA approval label, the _____ and the _____ .
6. The four types of containers or areas that are acceptable for storage of Top Secret information are:
- a. _____
 - b. _____
 - c. _____
 - d. _____
7. The three types of containers or areas acceptable for storage of Secret information are:
- a. _____
 - b. _____
 - c. _____
8. A key-operated lock is used in the storage of Secret bulky material. The lock's key must also be treated as if it were classified Secret.
- True False
9. You are going to procure new storage equipment. The _____ lists those items that you can procure.
10. Storage containers will display a label indicating the level of classified information stored in the container.
- True False

11. The four occasions when lock combinations should be changed are:
- a. _____
 - b. _____
 - c. _____
 - d. _____
12. A GSA-approved security container has been damaged. To be considered repaired, strict standards must be met. If repair standards are not met, the _____ and the _____ must be removed. A container not meeting repair standards may be used only for storage of _____.
13. U.S. Government classified information in a foreign country may be stored in any structure as long as that structure has a GSA-approved security container.
- True False

SOLUTIONS AND REFERENCES

1. a. Inadvertent disclosure
b. Deliberate attempts to gain access (p. 7-3)
2. level of classification
local situations (p. 7-5)
3. a. Nature and size of the activity
b. Mission of the activity
c. Level and type of classified information (p. 7-6)
4. a. Containers
b. Vault doors
c. Modular vaults
d. Alarm systems
e. Associated security devices (p. 7-7)
5. test certification label
identification label (p. 7-9)
6. a. A GSA-approved security container with supplemental controls
b. A vault with IDS
c. A GSA-approved modular vault with IDS
d. A secure room with IDS (p. 7-11)
7. a. Those that meet Top Secret storage standards
b. GSA approved security container or vault w/o supplemental controls
c. Secure rooms (meeting Component standards established prior to 1 Oct 95)
(p. 7-13)
8. True. (p. 7-14)
9. Federal Supply Schedule (p. 7-15)
10. False. (p. 7-16)

11.
 - a. When the container or padlock is placed in use
 - b. When a person who knows the combination no longer needs access.
 - c. When the combination has been subject to possible compromise
 - d. When the container or padlock is taken out of service. (p. **7-17**)

12. test certification label
GSA approval label
unclassified materials (p. **7-19**)

13. False. U.S. classified in a foreign country may be stored only at:
 - a. A U.S. military installation, US embassy or consulate
 - b. At a building used exclusively by U.S. government tenants if the building is under 24-hour control by U.S. government personnel.
 - c. At a building not used exclusively by U.S. Government tenants with other restrictions dependent upon whether or not the host government controls the building. (p.**7-19**)