CHAPTER 11

SECURITY

As a Signalman, you will hear a great deal about the security of classified material. You will have access to and will use classified information every day. For that reason, all activities brief newly arrived Signalmen in security and require them to sign a statement attesting that they have received the briefing and understand the contents. Furthermore, as part of each command's security program, you will be required to read and indicate your understanding of several of the most important national laws and regulations related to security.

Maintaining the security of classified material, however, requires more than a briefing, a regulation, or a law. Security will only be as effective as you make it. There is no one to whom you can transfer your responsibility for protecting this information. Security, along with operating signaling equipment, is a basic part of your duties. You must be security conscious to the point that you automatically exercise proper discretion in the discharge of your duties, and do not think of security as something separate and apart from other matters. In this way, security of classified information becomes a natural element of every task, and not an additionally imposed burden.

PURPOSE OF SECURITY PROGRAM

LEARNING OBJECTIVES: Explain the purpose of the security program. Define command management, security education, and security principles.

The security program deals basically with the safeguarding of information that should not be allowed to fall into the hands of foreign governments, foreign nationals, or other unauthorized persons. The danger being that such information might be used to the detriment of the United States.

Information may be compromised through careless talk, improper handling of classified material, and in various other ways. Some of the ways in which military personnel may accidentally give away vital information are discussed in *Basic Military Requirements,* NAVEDTRA 12043.

COMMAND MANAGEMENT

Commanding officers are responsible for effective management of the Information and Personnel Security Program within their command. Command security management discussion includes the following action areas:

- Designating a security manager
- Designating a Top Secret control officer (TSCO) if Top Secret material is handled by the command
- Designating an ADP security officer if the command processes data or prepares documents in an automated system
- Designating a security officer
- Preparing written command security procedures and an emergency destruction plan for the protection of classified material
- Reviewing and inspecting the effectiveness of the program in subordinate commands

Command Security Manager

Every command in the Navy and Marine Corps eligible to receive classified information is required to designate a security manager in writing. The security manager will be afforded direct access to the commanding officer to ensure effective management of the command’s security program.

The security manager may be employed full-time, part-time, or as a collateral duty, but he/she must be an officer or a civilian employee GS- 11 or above. The security manager must be a U.S. citizen and have a favorably completed background investigation (BI).

The security manager is the main advisor on information and personnel security in the command and is responsible to the commanding officer for the management of the program.

The security manager, for effective management of the program, should do the following:

- Develop written command information and personnel security procedures, including an emergency destruction plan.

- Formulate and coordinate the command's security education program.
- Ensure that threats to security, compromises, and other security violations are reported, recorded and, when necessary, investigated.
- Administer the command's program for classification, declassification, and downgrading of classified material.
- Maintain liaison with the public affairs officer to ensure that proposed press releases do not contain classified information.
- Ensure compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction, and disposition.

The duties of the security manager are numerous. Refer to *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1, for more information concerning his/her duties.

Top Secret Control Officer

Each command that handles Top Secret information must designate, in writing, a Top Secret control officer (TSCO). The person designated must be an officer, senior non-commissioned officer, or a civilian employee GS-7 or above. The TSCO must be a U.S. citizen with a Top Secret clearance.

The TSCO is responsible to the security manager for the receipt, custody, accounting for, and disposition of Top Secret material in the command. Procedures for the duties of the TSCO are set forth in OPNAVINST 5510.1.

Security Assistant

The security assistant must be a U.S. citizen and either an officer, an enlisted person E-6 or above, or a civilian employee GS-6 or above. The designation must be in writing. The assistant security manager does not require a BI unless he/she has been authorized to issue security clearances. The security assistant assists the security manager in his/her duties.

ADP/Information Systems Security Officer

Each command involved in processing data in an automated system must designate an ADP/IS security officer.

The ADP/IS security officer is responsible to the security manager for the protection of classified information being processed in the automated system and is responsible to the physical security officer for the protection of the personnel, equipment, and related resources.

SECURITY EDUCATION

Each command in the Department of the Navy (DON) that handles classified information will establish and maintain an active security education program to instruct all personnel, regardless of their position, rank, or grade, in security policies and procedures. The overall purpose of the security education program is to make sure that all personnel understand the need to protect classified information and know how to safeguard it.

Commanding officers, through their security managers, are responsible for security education in their commands, and for ensuring it is afforded a significant share of the time dedicated to command security.

SECURITY PRINCIPLES

The Department of Defense (DOD) security formula is based on the premise of circulation control (the control of dissemination of classified information). According to this policy, knowledge or possession of classified defense information is permitted only to persons whose official duties require access to the information ("need to know").

CLASSIFICATION CATEGORIES

LEARNING OBJECTIVES: Identify and define the classification designations and special markings.

Official information that requires protection in the interests of national security is placed into one of three categories: Top Secret, Secret, or Confidential. Following are examples and definitions of each category.

TOP SECRET

Top Secret is the designation applied only to information that requires the highest degree of protection. It is of such a nature that its unauthorized disclosure could reasonably be expected to cause

exceptionally grave damage to the national security, such as the following:

- An armed attack against the United States or its Allies
- The compromise of military or defense plans, intelligence operations, or scientific or technological developments vital to the national defense
- Disruption of foreign relations vitally affecting the national security

SECRET

Secret is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security, such as the following:

- Jeopardizing the international relations of the United States
- Endangering the effectiveness of a program or policy of vital importance to the national defense
- Compromising important military or defense plans, or scientific or technological developments important to national security
- Revealing important intelligence operations

CONFIDENTIAL

Confidential is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security, such as the following:

- Information that reveals strength of our land, air, or naval forces in the United States and overseas areas
- Documents and manuals containing technical information used for training, maintenance, and inspection of classified munitions of war
- Research, development, production, and procurement of munitions of war

MARKING

Classified material will be physically marked, annotated, or identified by means as prescribed in this section. The purpose of marking classified material is to inform the holder of the classification level and the degree of protection required, and to assist in extracting, paraphrasing, and downgrading and declassification actions. Therefore, all classified material must be marked in a manner that leaves no doubt about the level of classification assigned to the material.

Marking Requirenents

Marking requirements and the application of the markings vary depending on the kind of material. The following markings are required for all classified material:

Originally classified material

The identity of the original classification authority

The agency or office of origin

Declassification date

The overall classification

Any downgrading instructions

Derivatively classified material

The source of classification

The agency and office of origin

The overall classification

Declassification date

Downgrading actions

Publication Markings

The basic markings will be placed on the front of the publication. The overall classification will be placed at the top and bottom center of the front cover, title page, and first page. Downgrading and declassification instructions appear only on the face of the publication.

A back cover is not required; if used, the overall classification is placed at the top and bottom center.

The classification of each interior page (except blank pages) of a publication will be marked at the top and bottom center of the page. Normally, the overall classification of the publication is used. The marking of each interior page with the highest classification it contains, to include UNCLASSIFIED, is permissible. When marked in this manner, and the page is printed on the front and back, both sides of the page must be marked with the highest classification of either side. When one side contains information of a lower classification than the marking applied, a statement

such as “This page is unclassified” or “This page is Confidential” is used.

When a change is being issued to an existing classified publication, the changed pages will be marked as if they were already entered into the basic publication. If any of the changes is on an interior page, it will be marked in the same way as the interior pages of the basic publication.

Portion Markings

Each section, part, paragraph, or subparagraph of a classified document will be marked to show its level of classification or the fact that it is unclassified. The reason for this requirement is to eliminate any doubt as to which portion of the document contains, or can reveal, information requiring protection. The appropriate symbol will be placed immediately following a portion letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. The symbols are as follows:

- Top Secret (TS)
- Secret (S)
- Confidential (C)
- For Official Use Only (FOUO)
- Unclassified (U)

In addition to the classification symbols, the following symbols may also be used:

- Restricted Data (S-RD)
- Formerly Restricted Data (S-FRD)
- Critical Nuclear Weapons Design Information (S-RD) (N)

When a major numbered or lettered paragraph and all of its subparagraphs are unclassified, each paragraph need not be marked. Marking the lead-in paragraph with a (U) is sufficient.

The full classification—not the abbreviated form—is marked on figures, tables, graphs, charts, and so forth. The classification marking must be centered just below the illustration. Special situations may dictate the placement of the markings above or actually within the general area of the illustration. The important point is that the reader understand the classification level of that illustration.

COMPROMISES AND SECURITY VIOLATIONS

LEARNING OBJECTIVES: Define *compromises* and *security violations.* List some of the reasons that lead to compromises and security violations.

There are two types of security violations: Those that result in a confirmed compromise or possible compromise of classified information, and those that do not but in which a security regulation has been violated.

Compromise is the disclosure of classified information to a person who is not authorized access. The unauthorized disclosure may have occurred knowingly, willfully, or through negligence.

The compromise of classified information presents a threat to national security. The seriousness of the threat must be determined and action taken to reduce the effects of compromise. At the same time, action must be taken to investigate the circumstances and determine the causes, to prevent recurrence.

Compromise of classified material results when a security violation has resulted in confirmed or suspected exposure of classified information or material to an unauthorized person. The compromise is considered “confirmed” when conclusive evidence exists that classified material was compromised; it is considered “suspected” when some evidence exists that classified material has been subjected to compromise.

Any individual in the DON who is aware of the compromise or possible compromise of classified material must report the facts immediately to the most readily available command.

Individuals who are aware of possible acts of sabotage, espionage, deliberate compromise, or other subversive activities must report immediately all available information to the most readily available command, which, in turn, will notify the appropriate Naval Investigative Service office.

SECURITY CLEARANCES

LEARNING OBJECTIVES: Explain the purpose of security clearances. List and explain the types of BI done on an individual requiring a security clearance.

A personnel security clearance is an administrative determination that an individual is eligible for access to classified information of the same category as or lower than the clearance being granted.

No one will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of his/her loyalty, reliability, and trustworthiness. The initial determination will be based on a personnel security investigation (PSI) appropriate to the access required or to other considerations of the sensitivity of the duties assigned. Only the following personnel are authorized to request PSIs on personnel under their jurisdiction:

- Director, Central Adjudication Facility
- Commanders and commanding officers
- Chiefs of Recruiting stations

Request for PSIs must be kept to the absolute minimum. Reliance on PSIs as a means of identifying problem personnel security cases will be avoided. Special attention is to be given to eliminating unnecessary and duplicate reports. PSIs will not be requested to resolve allegations of a suitability nature for the purpose of supporting personnel administrative decisions or disciplinary procedures independent of a personnel security determination.

The Defense Investigative Service (DIS) or the Office of Personnel Management (OPM) conducts or controls all PSIs for the DON. DON elements are prohibited from conducting PSIs without a specific request from DIS to support its investigative responsibilities.

TYPES OF INVESTIGATIONS

The term *personnel security investigation* describes an inquiry by an investigative agency into an individual's activities for the specific purpose of making a personnel security determination. Investigations conducted for other purposes may have an impact on security clearances or assignments to sensitive duties, but are not PSIs. The following are some of the types of investigations. See *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1, for more information on PSIs.

National Agency Check

A national agency check (NAC) consists of a check of the files of a number of government agencies for pertinent facts bearing on the loyalty and trustworthiness of the individual. Examples of agencies checked are the FBI and the Defense Central Index of Investigations. The NAC conducted on a first-term enlistee in the Navy or Marine Corps is called an entrance NAC (ENTNAC). The primary reason for the ENTNAC is to determine the suitability of an individual for entry into the service. If a service member reenlists after a break in active service greater than 12 months, an NAC (not an ENTNAC) is requested.

Background Investigation

The background investigation (BI), conducted by DIS, is much more extensive than a NAC. It is designed to develop information as to whether the access to classified information by the person being investigated is clearly consistent with the interests of national security. It includes an NAC and probes deeply into the loyalty, integrity, and reputation of the individual.

Special Background Investigation

The special background investigation (SBI) is an investigation conducted by DIS, with extended coverage of the individual's background to provide a greater depth of knowledge than a BI. The scope of an SBI is 15 years or since the 18th birthday, whichever is shorter. At least 2 years will be covered, except that no investigation is conducted prior to the subject's 16th birthday.

CLEARANCE ELIGIBILITY

Eligibility for a security clearance is limited to members of the executive branch of the U.S. Government or to employees of the DOD contractors, under the Defense Industrial Security Program. Occasionally, it is necessary for the DON to clear persons outside the executive branch of the government. Only U.S. citizens are eligible for security clearances. Non-U.S. citizens may be considered for limited access authorization.

Classified information is made available to appropriately cleared persons only when it is necessary in the interests of national defense and the individual requires the information to carry out

assigned duties. Personnel authorized access to classified information must be trustworthy, loyal, and of good character.

In the following situations, a security clearance is not granted:

- To persons in nonsensitive civilian positions
- To persons whose regular duties do not require authorized access to classified information
- For ease of movement within a restricted, controlled, or industrial area of persons whose duties do not require access to classified information
- To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, police, and so forth
- To persons whose access to classified information can be prevented by a clear escort
- To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented
- To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures

Reserve personnel in an "active status" are eligible for a security clearance as required. Members of Congress do not require security clearances. They may be granted access to DOD classified information that relates to matters under the jurisdiction of the respective committees.

INTERIM AND FINAL CLEARANCES

Interim clearance may be granted only after the required investigative forms for final clearance have been sent to DIS or OPM and a check of available personnel, medical, legal, security, base police, and other command records do not contain information that clearly indicates that the individual is not a suitable candidate for a position of trust. Interim clearances are effective up to 6 months and may be extended another 6 months if a tracer has confirmed that the investigation is still pending.

A final clearance is granted upon completion of all investigative requirements as set forth in *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1.

ACCESS

No one has a right to have access to classified information solely because of rank, position, or security clearance. The final responsibility for determining whether a person's official duties require access to any element or item of classified information and whether he/she has been issued the appropriate security clearance or authorization by proper authority rests with the individual who has the authorized possession, knowledge, or control of the information involved—not with the prospective recipient.

The ultimate authority for granting access to classified information rests with the commanding officer, who is responsible for the security of the information or material in his/her command. A commanding officer may grant access to classified information to an individual who has an official need to know, a valid security clearance or access authorization, and about whom there is no locally available disqualifying information.

More in-depth information concerning access to classified information and material is covered in chapter 24 of OPNAVINST 5510.1.

STORAGE OF CLASSIFIED MATERIAL

LEARNING OBJECTIVES: Explain the procedure for the storage of classified material. Define *security container* and explain requirements when keys and combinations to containers are used.

Commanding officers are responsible for safeguarding all classified information within their commands and for ensuring that classified material not in actual use by appropriately cleared personnel or under their direct personal observation is properly stored.

Any weakness in equipment being used to safeguard classified material in storage is reported to the Chief of Naval Operations. Each report must fully describe the weakness or deficiency and how it was discovered. Reporting is especially important when GSA-approved containers are involved.

Valuables, such as money, jewels, and so forth, will not be stored in the same containers used to safeguard classified material. These items increase the risk that the container will be opened or stolen, with the resulting compromise of the information within.

Table 11-1 identifies the minimum requirement for storing classified material. It must be used in evaluating the security container and supplemental control required to properly safeguard classified information stored within.

STORAGE

Top Secret material will be stowed in a class A or B vault, a strongroom that meets the prescribed standards, or a General Services Administration (GSA) approved security container. When located in a building, structural enclosure, or other areas not under U.S. Government control, the vault, strongroom or security container must be protected by an alarm system or guarded by U.S. citizens during nonoperating hours or located in an alarmed area that affords protection equal to or better than that prescribed. When an alarm is used, the physical barrier must be adequate to prevent the following actions:

- Surreptitious removal of the material
- Observation that would result in compromise of the material

The physical barrier must be such that forcible attacks will result in evidence of attempted entry into the room or area. The alarm system must, at a minimum, provide immediate notice to a U.S. security force of an attempted entry.

Secret and Confidential material will be stored in the manner prescribed for Top Secret material or until phased out; in a steel filing cabinet having a built-in GSA-approved combination lock; or as a last resort, a steel filing cabinet equipped with a steel lockbar, secured by an approved GSA combination padlock When a lockbar container is used, the following procedures apply:

- The keeper and staples of the lockbar must be secured to the filing cabinet by welding, rivets, or peened bolts.
- The drawers of the container must be held securely closed when the lockbar is in place, so their contents cannot be removed by forcing open a drawer.
- During working hours, padlocks must be placed in the cabinet or locked through the staple until the cabinet is secured at the end of the day.

Table 11-1.—Storage Requirements

	SHORE INSTALLATIONS			SHIPS			AIRCRAFT		
	TS[1]	S	C	TS[1]	S	C	TS[1]	S	C
CLASS “A” VAULT	X	X	X						
CLASS “B” VAULT	X[2]	X	X						
STRONGROOM	X[3]	X[2]	X	X[5]	X[2]	X	X[5]	X[2]	X
GSA CONTAINER	X[2]	X	X	X[2]	X	X	X[2]	X[4]	X
LOCK BAR CABINET		X[2]	X[4]		X[2]	X		X[2]	X[4]
LOCKED CONTAINER OF SUBSTANTIAL METAL OR WOODEN CONSTRUCTION					X[6]	X[6]		X[6]	X[6]

[1] Must be located in buildings, ships, and aircraft that are under U.S. Government control; otherwise, must be protected by an alarm system or be guarded during non-working hours by U.S. citizens.

[2] Surrounding area locked and access to area controlled by U.S. personnel.

[3] Container alarmed or guarded by U.S. personnel.

[4] Surrounding area locked.

[5] Area alarmed and patrolled every hour by U.S. personnel.

[6] Surrounding area locked when not manned by U.S. personnel. Locked area must be checked every 24 hours.

- Precautionary measures must be taken so papers stored in the container will not protrude from the drawers when they are closed, or cannot be fished out through the cleft surrounding the drawers. One method is the insertion of stiff cardboard, such as a file folder, in a horizontal position above papers filed in the drawer.

Storage areas for bulky Secret or Confidential material must have access openings secured by GSA-approved combination padlocks or key-operated padlocks with high security cylinders. If these storage requirements cannot be met afloat or aboard aircraft, Secret or Confidential material may be stored in a locked container of substantial metal or wood construction secured by an approved GSA combination padlock. In this case, the area must be locked when not manned and checked at least once every 24 hours.

NEW STORAGE CONTAINERS

New security containers should not be procured until a physical security survey of existing equipment and a review of classified records on hand has been made. It might be determined that it would not be feasible to use the equipment or to retire, return, or declassify or destroy a sufficient volume of records currently on hand to make the needed security storage space available.

Only containers that have been approved by the Federal Government as security filing equipment should be procured. Equipment is selected from the National Supply Schedule of the GSA following the procedures outlined in SECNAVINST 10463.1. Modification of any equipment that is used to store classified material is prohibited. Exceptions to permit acquisition of special-purpose equipment or to modify filing cabinets to bar-padlock types suitable for storing classified material must be requested from the CNO.

A security container records form (fig. 11-1) will be maintained for each security container used for the storage of classified material. The container will be inspected each watch.

Security containers conforming to Federal specifications bear a test certification label on the locking drawer, attesting to the security capabilities of the container and lock.

NONAPPROVED SECURITY CONTAINERS

Nonapproved security containers are available in many shapes and sizes; however, containers of this type may not be used to store classified material even though they may be equipped with manipulation-proof or manipulation-resistant locks and have other security and fire protection features.

Nonapproved containers used to safeguard classified material should be replaced by an approved GSA security container.

COMBINATIONS

A security container, vault, or storeroom must be fitted with a lock that resists opening by unauthorized persons. Manipulation-resistant (MR) and manipulation-proof (MP) locks are tested by the Underwriters' Laboratory (UL) and must have the UL label attached to the back of the lock.

Federal specifications governing the manufacture of security containers and security vault doors require that the unit be equipped with a top-reading changeable combination lock that controls the locking of the container. The top-reading design replaced the front-reading design to provide increased protection against the combination being ascertained by covert viewing. Combination locks are available with two forms of combination changing: hand or key. Hand-changing requires removing the wheel pack and changing the wheel to the new combination. Key-changing requires the use of a key that is inserted into the lock case, permitting a new combination to be set. The type of combination lock desired should be specified when ordering the container.

The following requirements help ensure the effectiveness of combination locks:

1. Combinations must be changed only by individuals having the responsibility and an appropriate security clearance.
2. The combination will be given only to people whose official duties demand access to the container.
3. The combination to a security container is changed at the time the container is received, at the time any person having knowledge of the combination leaves the organization, at any time there is reason to believe that it has been compromised, or as a minimum every 24 months.

In selecting combination numbers, multiples of 5, simple ascending or descending arithmetical series, and personal data (such as birthdates and service numbers) should be avoided. The same combination will not be used for more than one container in any one component.

SECURITY CONTAINER RECORDS FORM
OPNAV FORM 5510/21 (10-70) S/N 0107-LF-783-5100

CONTAINER NUMBER	LOCATION	OFFICE CODE	TYPE OF CONTAINER (MAKE/SIZE)
0284	Room 750 CWB	CNO (Op-XXX)	Mosler/5 drawer legal
DATE RECEIVED	**CLASS OF CONTAINER**		**FEDERAL STOCK NUMBER**
(Date)	☐ CLASS 2 ☐ CLASS 3 ☐ CLASS 4 ☐ CLASS 5 ☒ CLASS 6		7110-91-9193
SERIAL NUMBER	**DATE OF MANUFACTURE**	**QUANTITY OF DOCUMENTS**	**SCOPE OF MATERIAL**
16155	(Date)	10 linear feet	Confidential - Secret

SECURITY POINTS FOR CONTAINER	OTHER SECURITY POINTS	TOTAL SECURITY POINTS

PERCENTAGE OF CLASSIFIED MATERIAL STOWED

TOP SECRET 0% SECRET 65% CONFIDENTIAL 35% UNCLASSIFIED 0%

TYPE OF LOCK (MAKE/MODEL)	SERIAL NUMBER (IF APPLICABLE)	
	HASP	LOCK CASE
Mosler Handchange		

CONDITION OF CONTAINER

Good

REMARKS

See reverse

FRONT

OPNAV FORM 5510/21 (10-70) (BACK)

INSPECTION AND REPAIR

DATE INSPECTED	INSPECTED BY	CONDITION	REPAIRS MADE/DRILLED
(Date)	Rbc	NEW	
(Date)	SCW	LOCKOUT	Drawer head replaced (Date)

BACK

8GNP0231

Figure 11-1.—Security Container Records form, OPNAV Form 5510/21.

In setting a combination, numbers should be used that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

To prevent lockout, two people should try a new combination before closing the container or vault door.

The combination of a vault or container will be assigned a security classification equal to the highest category of the classified material authorized to be stored in it. Records of combinations shall be sealed in an envelope and kept on file by the security manager, duty officer, communications officer, or other persons designated by the commanding officer.

KEYS

When key-operated high-security padlocks are used, keys will be controlled at the level of the highest classification of material being protected. The following safeguards will also be used:

- A key and lock custodian for custody and handling of keys will be appointed.
- A key and lock control register that identifies keys for each lock and where and by whom they are held will be maintained.
- Keys and locks will be audited each month and a written record of each inventory will be made.
- Keys will be inventoried each time custody changes.
- Keys will not be allowed to be removed from the command.
- Keys and spare locks will be stored in a locked security container.
- Locks will be changed or rotated at least annually and replaced if their keys are lost or subjected to compromise.
- Master keying is prohibited.

A record for each vault, secure room, or container used for storing classified material will be maintained showing the location of the container, and the names, home addresses, and telephone numbers of persons having knowledge of the combinations. Standard Form 700 (fig. 11-2) is used for this purpose.

SECURING A SECURITY CONTAINER

When securing a security container, rotate the combination dial at least four complete turns in the same direction. In most locks, if the dials are given only a quick twist, it is possible to open the lock merely by turning the dial back in the opposite direction. Each drawer of the container and file cabinets will be checked to make sure the equipment has been secured.

REPAIRING SECURITY CONTAINERS

Lockouts or repair of any damage that affects the integrity of a security filing cabinet approved for storage of classified material will only be done by appropriately cleared or continuously escorted personnel.

A GSA-approved security file cabinet is considered to have been restored to its original state of security if all damage or altered parts are replaced

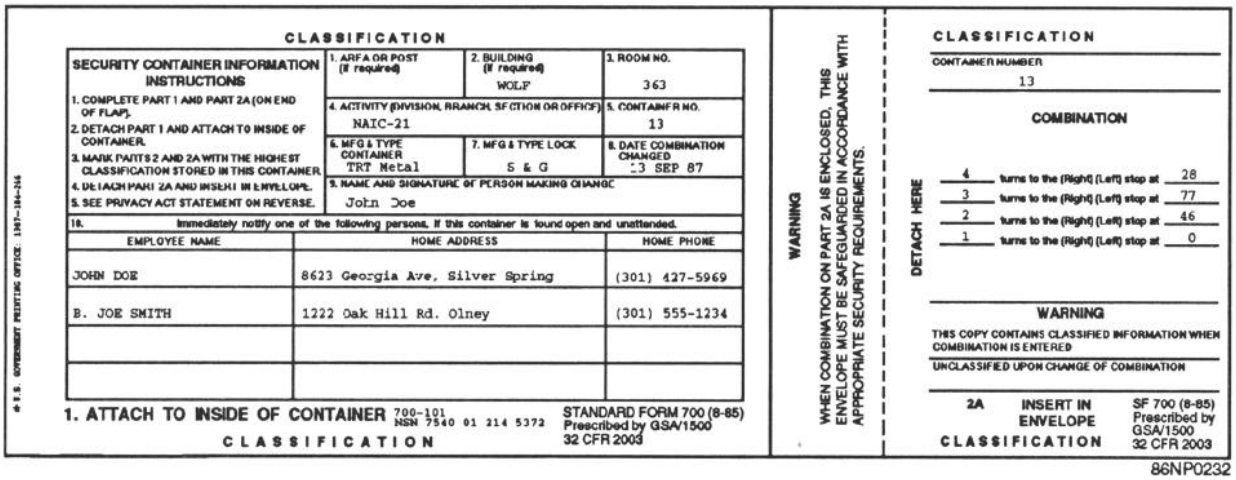


Figure 11-2.—Security Container Information form, Standard Form 700.

with new cannibalized parts. A container that has been drilled immediately adjacent to or through the dial ring to neutralize a lockout should be restored in the following manner: The replacement lock is equal to the original equipment; the drilled hole is repaired with a tapered case-hardened steel rod with a diameter slightly larger than the hole. The outside of the drawer must be puttied, sanded, and repainted so no visible evidence of the hole or its repair is noticeable.

SAFEGUARDING

LEARNING OBJECTIVES: Explain the procedures for safeguarding classified information. Explain restricted area, the care of working spaces, the care to be taken during working hours, and security checks to help safeguard classified information.

Classified information or material will be used only where there are facilities, or under conditions, adequate to prevent unauthorized persons from gaining access to it. Where possible, classified holdings will be consolidated to limit the area where they will be used.

Anyone who has possession of classified material is responsible for safeguarding it at all times, and particularly for locking classified material in appropriate security equipment whenever it is not in use or under supervision of authorized persons. The custodian must follow procedures that ensure unauthorized persons do not gain access to classified information by sight or sound or other means. Classified information will not be discussed with or in front of unauthorized persons.

A custodian will not remove classified information or material from designated office or working areas except in the performance of his/her official duties and under conditions providing the protection required by OPNAVINST 5510.1.

Under no circumstance is a custodian to remove classified material from designated areas for the purpose of working on such material during off-duty hours or for other purposes involving personal convenience unless specifically approved by the Chief of Naval Operations, a fleet commander in chief, the commander of the Naval Space Command, the commanders of the Naval System Commands, the Chief of Naval Research, the Commandant of the Marine Corps, or the Commanding General of Fleet Marine Force Atlantic or Pacific. Approval will be given only when there is an overriding need; when the required physical safeguards, including a GSA-approved container, are met; and when a list of all the material removed is kept at the command.

RESTRICTED AREAS

Depending on the nature of the work, information, equipment, and material concerned, different areas within a command may have varying degrees of security. To meet this situation, the command should apply different protective measures.

To provide for an effective and efficient method to restrict access and to control movement where classified material is stored or used, such areas will be designated Restricted Areas and only those persons whose duties actually require access and who have appropriate security clearances will be allowed freedom to move within the area. Persons not having the proper clearances may, with appropriate approval, be admitted into an area, but they must be controlled by an escort.

Restricted Area warning signs will be posted at all normal points. When a language other than English is prevalent, warning signs will be in both English and the local language.

CARE DURING WORKING HOURS

During working hours, precautions should be taken to prevent access to classified information by unauthorized personnel. Among the necessary precautions to be followed are the following:

- When classified documents are removed from storage for working purposes, they are to be kept under constant surveillance, face down or covered when not in use. Cover sheets will be Standard Forms 703, 704, or 705 respectively, for Top Secret, Secret, and Confidential documents.

- Classified information will be discussed only when unauthorized persons cannot overhear the discussion. Particular care should be taken when there are visitors or workmen present. Escorts should alert fellow workers when visitors or workmen enter the space.

- Drafts, carbon sheets, carbon paper, typewriter ribbons (one-time), plates, stencils, stenographic notes, worksheets, and similar items containing classified information are either destroyed by the person responsible for the preparation of material after they

have served their purposes, or are given the same classification and safeguarded in the same manner as the classified material produced with them.

- New typewriter ribbons used in the preparation of classified material are either typed on until illegible or given the same classification and safeguarded in the same manner as the classified material prepared with them.

- Personnel will not normally be permitted to work alone in areas where Top Secret information or information controlled under special access program procedures is used or stored and is accessible to those employees. This policy, the two person integrity requirement, does not apply in those situations where one individual is left alone for a brief period during normal duty hours. It does not require both individuals to have equal access or that a "no lone zone" be established around Top Secret areas, nor is the requirement as stringent as the two-person control requirement for the Communication Material System (CMS). Outside normal duty hours, strict adherence to two-person integrity will be followed.

SECURITY CHECKS

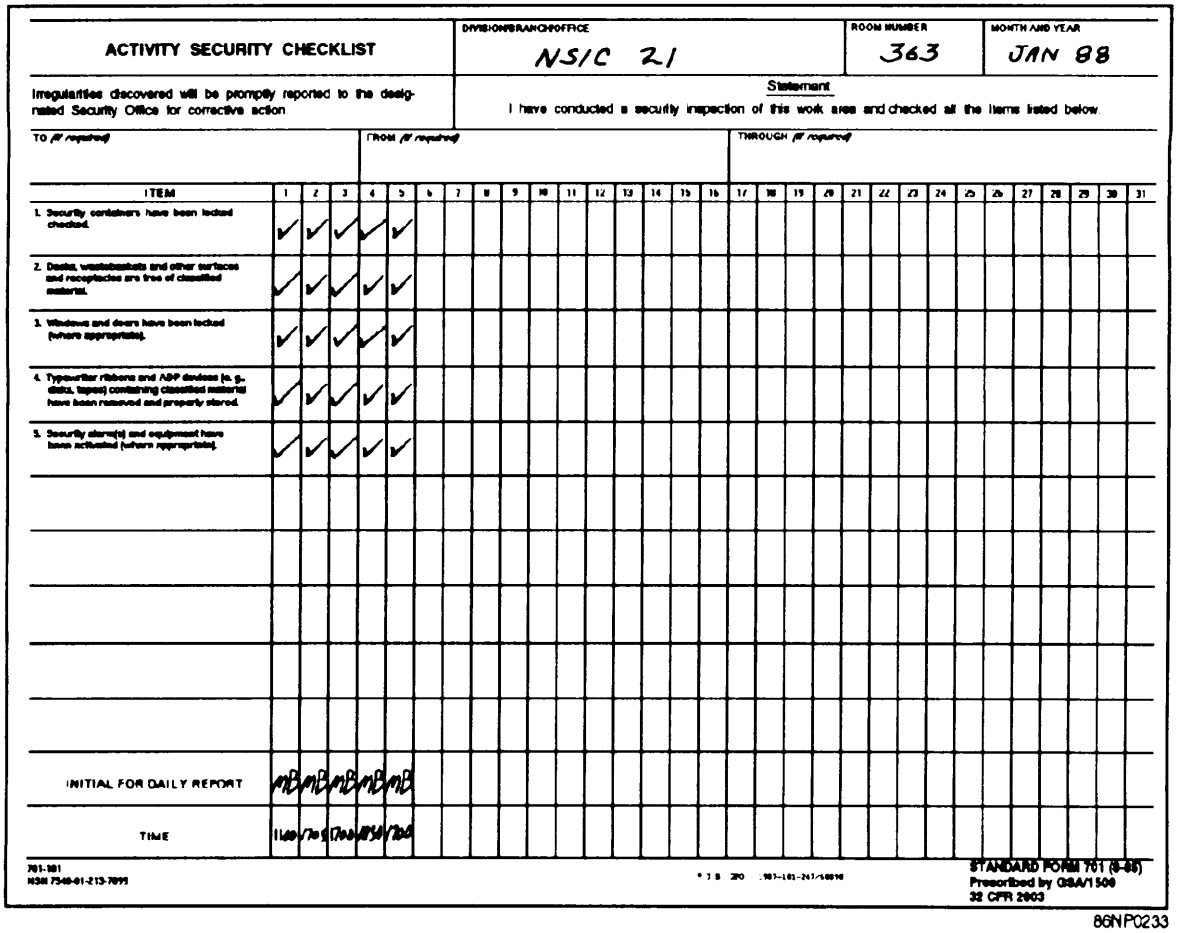
Commanding officers must require a security check at the end of each working day to ensure that all classified material is properly secured, and that Standard Forms 701 and 702 (figs. 11-3 and 11-4) are used. The security check determines the following:

- All classified material is stored in the manner prescribed.

- Burn bags are properly stored or destroyed.

- The contents of wastebaskets that contain classified material have been properly stored or destroyed.

- Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stored or destroyed.



ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE: NSIC 21

ROOM NUMBER: 363

MONTH AND YEAR: JAN 88

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 the items listed below.

TO (If required) | FROM (If required) | THROUGH (If required)

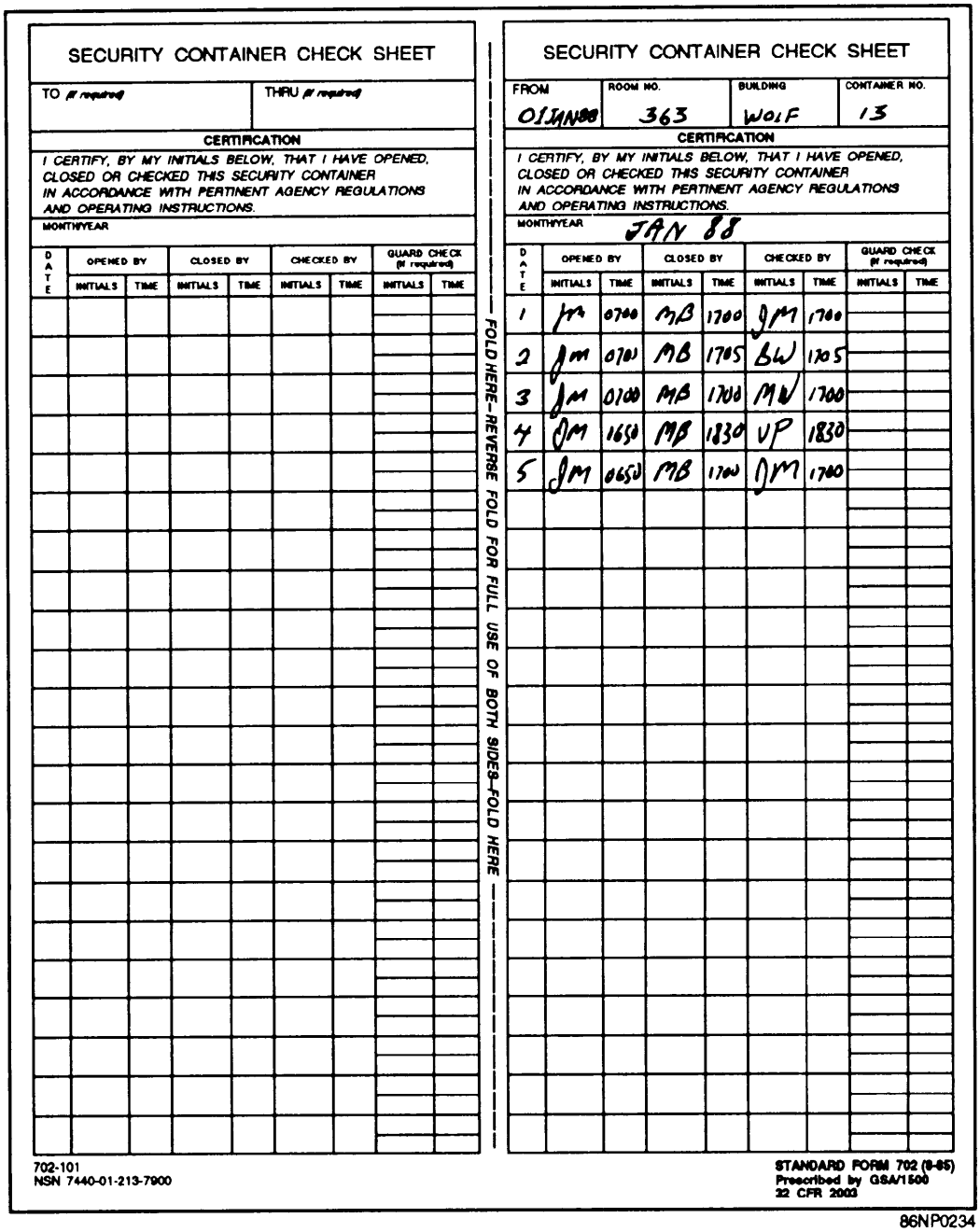
ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.	✓	✓	✓	✓	✓																										
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.	✓	✓	✓	✓	✓																										
3. Windows and doors have been locked (where appropriate).	✓	✓	✓	✓	✓																										
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.	✓	✓	✓	✓	✓																										
5. Security alarm(s) and equipment have been activated (where appropriate).	✓	✓	✓	✓	✓																										
INITIAL FOR DAILY REPORT	mB	mB	mB	mB	mB																										
TIME	1140	730	1700	0754	1700																										

701-101
NSN 7540-01-213-7899

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

8GNP0233

Figure 11-3.—Activity Security Checklist, Standard Form 701.



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.
01JAN88	363	WOLF	13

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 JAN 88

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (If required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
1	JM	0700	MB	1700	JM	1700		
2	JM	0701	MB	1705	BW	1705		
3	JM	0100	MB	1700	MB	1700		
4	JM	1650	MB	1830	VP	1830		
5	JM	0650	MB	1700	JM	1700		

702-101
NSN 7440-01-213-7900

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

86NP0234

Figure 11-4.—Security Container Check Sheet, Standard Form 702.

• Security containers have been locked by the responsible custodians, and the dial of combination locks has been rotated at least four complete times in the same direction in securing safes, files, or cabinets.

CARE OF WORKING SPACES

At a shore establishment, the precautions taken to protect classified information include trimming shrubbery outside ground floor offices that would afford cover for possible prowlers, and installing heavy-duty grilles, screens, or bars on ground floor windows and other accessible openings if the building is in an exclusion or limited security area. The protective grilles and screens have the additional value of preventing missiles such as hand grenades and incendiaries from being hurled through the windows from outside the perimeter.

Classified information should not be disclosed through conversations. Inspections of spaces should be made for unauthorized wiring and possible concealment of listening devices in such places as

behind pictures and radiators, and under desks. Repairs, routine maintenance, and cleaning in sensitive areas should be performed by reliable personnel under supervision.

DECLASSIFICATION, DOWNGRADING, AND UPGRADING

LEARNING OBJECTIVE: Explain the procedures for declassification, downgrading, and upgrading of classified information.

DECLASSIFICATION/DOWNGRADING

Information classified by the DON will be declassified as soon as national security considerations permit. Declassification or downgrading must be based on the loss of sensitivity of the information with the passage of time or the occurrence of an event that permits declassification or downgrading.

The following officials are authorized to declassify or downgrade classified information:

- Secretary of the Navy
- The original classification authority, his/her successor, or a superior of either
- The deputies or chief of staff to those original classification authorities for classified information within their functional areas
- The director of Navy history and the director of Marine Corps history and museums, in coordination with original classification authorities, for historical records in their custody

The above mentioned officials are the only ones who can decide that certain information no longer requires the protection originally assigned. The authority to declassify or downgrade is not to be confused with the administrative responsibility of a holder of classified information to declassify or downgrade it as directed by a classification guide, the continued protection guidelines, or the instruction on a document.

TRANSFERRED MATERIAL

When classified material is officially transferred from one command to another, the receiving commanding officer, if he/she is a designated authority, becomes the declassification and downgrading authority over the material. If the commanding officer is not designated, the next senior official in his/her command will be responsible for declassification and downgrading.

When practicable, material will be reviewed for declassification or downgrading before it is sent to records centers or to the national archives for storage.

UPGRADING

Authorities may upgrade classified information within their functional areas only when:

- all known holders of the information can be promptly notified; and
- all known holders of the information are authorized access to the higher level of classification, or the information can be retrieved from the known holders not authorized access to the higher level of classification.

Information previously determined to be unclassified may be classified only when the original classification authority determines that correct criteria has been met, that control of the information has not been lost, and that loss of control can still be prevented.

If classified information is, through administrative or other error, disseminated as unclassified or is underclassified, every effort will be made to retrieve, safeguard, and properly mark and control the information.

NOTIFICATION

Notices are not issued to declassify or downgrade material marked with specific events for declassification or downgrading. All original addressees will be notified, however, of an unscheduled change to shorten or lengthen duration of or to change the classification level. A notice assigning classification to currently unclassified information will be classified Confidential unless the notice itself contains information at a higher level. The notice declassification date will be no less than 90 days from the date of the notice.

ACCOUNTING AND CONTROL

LEARNING OBJECTIVE: Explain the procedures for the accounting and control of Top Secret, Secret, and Confidential material.

The accounting system for an activity should provide readily available information on what classified material it has received, what classified material it has produced, and who has custody of the material.

The control of classified material is necessary for several purposes. It must be controlled (1) to limit dissemination and to prevent excessive production or reproduction; (2) so that when the material is regraded or declassified, the holder or recipients can be determined and notified; and (3) so that the office or person normally responsible for its security can be determined.

Top Secret Material

The command TSCO is responsible for receiving, maintaining, distributing, and destroying Top Secret documents. All Top Secret material received by a command will be entered into the command's accountability register. This register will identify each Top Secret document, including the changes, show the number of copies, and give the disposition of each copy. The register will be retained for 5 years after the documents are transferred, downgraded, or destroyed.

All Top Secret documents and equipment will be serially numbered at the time of origination. Additionally, each document will be marked to indicate its copy number as follows:

Copy No.____of ____copies

Top Secret documents must contain a list of effective pages and include a record of page checks. When that is impracticable, as in correspondence or messages, the pages shall be numbered as follows:

Page ____ of____pages

Retention of Top Secret documents will be kept to a minimum. Nonrecord documents will be destroyed as soon as their intended purpose has been served. When Top Secret documents are destroyed, a record of destruction will be prepared identifying the material destroyed and the two officials who witnessed the destruction. Top Secret documents that cannot be destroyed will be reevaluated and, when appropriate, downgraded, declassified, or retired to designated records centers.

Top Secret material may not be reproduced without the permission of the issuing office or higher authority; and when copies are made, each will be annotated to show its copy number.

A disclosure record, which shows the document title, the names of all individuals who have been afforded access to the document, and the date of access, must be maintained for each Top Secret document. Those in the command who may have access to containers in which Top Secret information is stored or who regularly handle large volumes of Top Secret information need not be included in the disclosure records. Disclosure records will be maintained for 5 years after the information has been downgraded, the document has been destroyed, or custody has been transferred.

The control of Top Secret information is maintained by the TSCO, if one is designated, or the classified material control officer. You may be required to assist either of them.

Secret Material

As a minimum requirement, commands must establish administrative procedures for recording all Secret material originated by, received and distributed or routed to components of or activities within the command, or disposed of by the command by transfer of custody or destruction. Records will be retained for at least 2 years.

Confidential Material

There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material. Administrative provisions are required, however, to protect Confidential information from unauthorized disclosure by access control and by compliance with the regulations on marking, storage, transmission, and destruction.

DISPOSITION OF CLASSIFIED MATERIAL

LEARNING OBJECTIVE: List procedures for the disposition of classified material when an individual is separated, dies, deserts, is relieved, or is missing in action.

When military or civilian personnel are separated from the DON, all classified material held by them is turned in to the source from which it was received, to their commanding officer, or to the nearest naval command, as appropriate, prior to delivery of final orders or separation papers.

A person about to be relieved will deliver to his/her successor all classified material in his/her custody. Appropriate receipts will be completed covering the change of custody for all Top Secret material. Classified material required by an individual at his/her next duty station, when approved, may be officially transferred.

When an individual dies, deserts, or is declared missing in action, the commanding officer, in disposing of the personal effects, makes sure no classified material is contained in the effects. Every effort will be made to recover classified material known to have been in possession of the person. Material not recovered or not known to be destroyed will be reported as a possible compromise.

DISSEMINATION

LEARNING OBJECTIVE: List procedures for the dissemination of classified material.

Commanding officers establish procedures for the dissemination of classified information originated or received by their command to limit outside dissemination to those activities having a need to know and to reflect any restriction imposed by originators or higher authority. Commanding officers also ensure that material prepared or submitted for public release does not contain classified information or proscribed technical data.

Except where specifically permitted, classified material originating in a non-DOD department or agency will not he disseminated outside the DOD without consent of the originating department or agency.

TOP SECRET

Top Secret material originated within the DOD will not be disseminated outside the DOD without consent of the originating department or agency, or higher authority.

SECRET AND CONFIDENTIAL MATERIAL

Secret or Confidential material originated within the DOD may be disseminated to other departments and agencies of the executive branch of the government unless specifically prohibited by the originator.

DISTRIBUTION

The distribution of classified material must be limited to those persons whose official duties require them to have knowledge or possession of such material. Responsibility for determining whether a person's duties require access to classified information and that the person is authorized to receive it rests upon each individual who has possession, knowledge, or control of the information involved.

The existence, nature, content, or whereabouts of classified information must not be divulged needlessly.

Classified material may be distributed to all agencies of the executive branch of the government. On requests from DOD agencies, the "need-to-know" may be judged on the face of the request. When the "need-to-know" is not discernible from the scope of the requester's activities, the need must be determined. Classified material sent to other activities of the executive branch of the government must be sent via the departmental headquarters of the requesting activity for a determination of "need-to-know" and capability to handle classified material.

No person in the DON is to convey orally, visually, or by written communication any classified information outside the executive branch of the government of the United States unless such disclosure has been specifically authorized by the CNO.

Classified information must not be discussed over telephones because of insecurity resulting from executive cut-in, phantom voice interceptions, and wiretapping. Telephones located in sensitive areas must be provided with a means of complete disconnection, such as a plug or jack arrangement if they are considered safe. Intercom systems located in sensitive areas must be confined to the sensitive area.

DESTRUCTION OF CLASSIFIED MATERIAL

LEARNING OBJECTIVE: Explain the procedures for the destruction and emergency destruction of classified material.

Top Secret, Secret, and Confidential material may be destroyed by burning, pulping, pulverizing, or

shredding, provided the destruction is complete and reconstruction is impossible. The destruction of Top Secret and Secret material will be recorded. Destruction may be recorded on OPNAV Form 5511/12 or on any other record that includes complete identification of the material, the number of copies destroyed, and the date of destruction. Destruction must be witnessed by personnel having a security clearance at least as high as the category of material being destroyed, and those witnesses must be thoroughly familiar with regulations and procedures for safeguarding classified information. Two officials will be responsible for the destruction of Top Secret and Secret material and will sign the record of destruction. Records of destruction will be retained for a period of 2 years.

When Top Secret or Secret material is placed in a burn bag, the witnessing official signs the record when the material is actually placed in the burn bag. Burn bags containing classified material must be safeguarded according to the classification of the material therein. When the burn bags are destroyed, the destruction must be witnessed by two appropriately cleared personnel. The persons accomplishing the actual destruction need not sign the record of destruction, but it would be appropriate to require a signature for the number of burn bags destroyed. All burn bags will be serially numbered, and a record will be kept of all handling until destroyed. The two persons actually doing the destroying will sign the record of handling. The record of handling will be retained for 2 years.

Confidential material and classified waste are destroyed by authorized means by appropriately cleared personnel, but these materials do not require a record of destruction.

Assignment to the destruction detail will be rotated periodically. Both personnel will be cleared to the highest level of information being destroyed. They must be familiar with the regulations and procedures for safeguarding classified information.

EMERGENCY DESTRUCTION

Commands located outside the United States and its territories, all deployable commands, and all commands holding COMSEC material must include in their emergency plan the destruction of classified material. Emergency destruction plans must be practical and reasonable and take into account the following factors:

- The level and sensitivity of classified material held by the activity
- The proximity of land-based commands to hostile or potentially hostile forces
- Flight schedules or ship deployments in the proximity of hostile or potentially hostile forces or potentially hostile environments
- The sensitivity of operation assignment (contingency planning should also be considered)
- The size and armament of land-based commands and ships
- The potential for aggressive action of hostile forces

Effective emergency planning includes the following measures:

- Reducing the amount of classified material held to the absolute minimum.
- Storing less frequently used classified material at more secure commands.
- To the extent possible, transferring retained material to magnetic media, which is more easily destroyed than paper. This precaution will also reduce the bulk that needs to be evacuated or destroyed.

The emergency destruction plan will emphasize the procedures and methods of destruction. It will clearly identify the exact location of all classified material. The plan will include priorities for destruction, billet designations of personnel responsible for destruction, and the prescribed place and method of destruction.

The emergency destruction plan will authorize the senior individual present in a space to deviate from established plans when situations warrant. It will also identify the individual who is authorized to make the determination as to when emergency destruction is to begin and the means by which this determination is to be communicated to all subordinate elements maintaining classified information.

Emergency destruction drills will be conducted at least annually to ensure that personnel concerned are familiar with the plan and associated equipment. Records of drills will be maintained for 2 years.

Emergency destruction falls into three priority classes: priority one, two, and three. These priorities will be based on the potential effect on national

security should holdings fall into hostile hands. The priorities are as follows:

Priority One—Top Secret material

Priority Two—Secret material

Priority Three—Confidential material

The requirement for priority-one material is that it must be destroyed first, with a time objective as follows:

Shore stations—60 minutes

Afloat stations—30 minutes

Aircraft—3 minutes

METHODS OF EMERGENCY DESTRUCTION

Classified material may be jettisoned at sea at depths of 1,000 fathoms or more. If such water depth is not available and if time does not permit other means of emergency destruction, the material should, nonetheless, be jettisoned to prevent its easy capture. When shipboard emergency destruction plans include jettisoning, document sinking bags shall be available. If a vessel is to be sunk through intentional scuttling or is sinking due to hostile action, classified material should be locked in security filing cabinets or vaults and allowed to sink with the vessel rather than attempting jettisoning.

Other means of emergency destruction include dismantling or smashing metallic items beyond reconstruction by available means such as sledge hammers, cutting tools, and torches; and supplementing emergency destruction devices with routine destruction equipment when time and circumstances permit. As a last resort and where none of the methods previously mentioned can be employed, use other means, such as dousing the classified material with a flammable liquid and igniting it; for instance, throwing all your classified material in the flagbag and igniting it.

REPORTING EMERGENCY DESTRUCTION

Accurate information concerning the extent of emergency destruction of classified material is second in importance only to the destruction of the material itself. Accordingly, the facts surrounding the destruction shall be reported to the CNO and other interested commands by the most expeditious means available. Reports are to contain the following information:

- Identification of the items of classified material that may not have been destroyed
- Information concerning classified material that may be presumed to have been captured
- Identification of all classified material destroyed and the methods of destruction

Additionally, within 6 months after the destruction, a written statement describing the character of the records and showing when and where the destruction was accomplished will be submitted to the Commander, Naval Data Automation Command.

The requirement for reporting of the emergency destruction of classified material shall be included as a part of the command's emergency plan.

SUMMARY

In this chapter, you learned the importance of security. You learned the purpose of the security program and the different classification categories. You learned what a compromise is and how to obtain a security clearance. You learned about the storage of classified material and the custodial precautions. You also learned how to destroy classified material and the procedures for reporting destructions. Security is a major part in running an effective signalbridge. So take a little time and learn your security!