CHAPTER 22

SECURITY REQUIREMENTS AND INTERNATIONAL AGREEMENTS

There is no way of estimating how many battles have been lost, how many ships have been sunk, or how many lives have been sacrificed because someone intentionally or unintentionally betrayed a military secret.

—Author unknown

Security is the safeguarding of classified information in the interest of national security. The safety of the United States in general and naval operations in particular depends on protecting classified material.

SECURITY

Learning Objectives: When you finish this chapter, you will be able to—

- Recognize the basic security policies, requirements, and procedures for handling classified material and information to include security classification and protection.
- Recall the procedures and principles involved in applying for personnel clearances.
- Identify the various classified material markings.
- Recognize the purpose of downgrading and declassifying classified material.
- Recall the procedures used to transmit classified material.
- Identify the basic security requirements concerning classified information and material and their security levels.
- Identify the types of equipment/material covered by automated data processing (ADP) security.
- Identify the terms used to describe the compromise of classified material.
- Recognize the procedures used to report a suspected compromise or a security violation.
- Identify the basic personal censorship requirements concerning classified information and material.
- Identify the procedures for reporting subversive activities on station or in a leave or liberty status.
- Identify when and where terrorism can occur.
- Identify the most common forms of terrorism.
- Recognize the terms *bomb threat* and *bomb incident*.
- Recall the procedures to follow when a bomb threat is received.

Security involves more than safeguarding classified printed information, such as photographs, blueprints, manuals, and charts. Security also includes safeguarding communications, such as mail, visual signals, radio transmissions, ship movements, or telephones. It includes anything that affects the security of our government in domestic and foreign affairs. It involves protection against sabotage, subversion, or any other illegal acts designed to weaken or destroy the United States. It's important for you to understand what classified information is and how to safeguard it.

Student Notes:

SECURITY CLASSIFICATION LEVELS

All information or material considered vital to the safety of the United States is given a security classification level. Each security classification level indicates (tells) the amount of protection the information and material requires to safeguard it against unauthorized disclosure. There are only three security classification levels—Top Secret, Secret, and Confidential.

The Secretary of the Navy (SECNAV) or his/her designees have the authority to originally classify information as Top Secret, Secret, or Confidential. The SECNAV's designees are listed in the *Department of the Navy Personnel Security Program,* SECNAVINST 5510.30A and *Department of the Navy (DON) Information Security Program (ISP) Regulation,* SECNAVINST 5510.36.

Top Secret

Top Secret is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause **exceptionally grave damage** to the national security. Some examples of information that could cause grave damage to national security include—

- Armed hostilities against the United States or its allies
- A disruption of foreign relations vitally affecting the national security
- The compromise of vital national defense plans
- The disclosure of complex cryptographic and communications intelligence systems
- The disclosure of sensitive intelligence operations
- The disclosure of significant scientific or technological developments vital to national security

Secret

Secret is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause **serious damage** to the national security. Some examples of information that could cause serious damage to national security include information that could—

- Disrupt foreign relations significantly affecting the nation's security
- Significantly impair a program or policy directly related to the national security
- Disclose significant military plans or intelligence operations
- Compromise significant scientific or technological developments relating to national security

Confidential

Confidential is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause **damage to** the national security. Some examples of information that could cause damage to national security include information that could—

- Indicate ground, air, and naval forces (such as force levels and force dispositions)
- Reveal performance characteristics, such as design, test, and production data of U.S. munitions and weapons systems

Controlled Unclassified Information

Controlled unclassified information is defined and governed by laws, international agreements, and regulations that address the identification, marking, protection, handling, transmission, transportation, and destruction of controlled unclassified information. Controlled unclassified information includes—

- For Official Use Only (FOUO) information under the Freedom of Information Act (FOIA)
- Department of State (DOS) Sensitive But Unclassified (SBU) information
- DOD and DOE Unclassified Controlled Nuclear Information (UCNI)

Student Notes:

- Drug Enforcement Administration (DEA) Sensitive Information
- Sensitive Information as defined by the Computer Security Act of 1987
- Unclassified information in technical documents requiring distribution statements and unclassified NNPI

SECURITY CLEARANCES

Sailors in many Navy ratings require some access to classified information. The commanding officer (CO) determines your need for a security clearance. The CO bases your need for a security clearance on your assignment at his/her command or potential assignment on transfer. To apply for a security clearance, you must be a U.S. citizen. There is a security investigation made on each Sailor needing a clearance. This investigation determines the Sailor's potential to protect information during the course of his/her duties.

Security clearances are granted to Sailors when their conduct and behavior are such that they can be entrusted with classified information or they can be assigned to sensitive duties. These are Sailors who—

- are loyal to the United States,
- comply with laws,
- have demonstrated dependability in accepting and discharging responsibilities,
- demonstrate good social adjustment and emotional stability, and
- have the ability to exercise sound judgment in meeting adversity.

To receive and keep a security clearance, you must have and maintain a good record. Your commanding officer can suspend a clearance if you don't maintain a good record. According to *Department of the Navy Personnel Security Program*, SECNAVINST 5510.30A, your command must report any of the following to the DON Central Adjudication Facility (CAF) (the DON CAF grants or revokes clearances):

- Involvement in activities or association with people who unlawfully practice or advocate overthrow or alteration of the United States government by unconstitutional means
- Foreign influence concerns or close personal association with foreign nationals or countries
- Foreign citizenship (dual citizenship) or foreign monetary interests
- Bad conduct, such as excessive drinking, gambling, promiscuity, or illegal or improper drug use/involvement
- Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security processing
- Unexplained affluence or excessive indebtedness
- Apparent mental, emotional, or personality disorder(s)
- Criminal conduct
- Noncompliance with security requirements
- Engagement in outside activities that could cause a conflict of interest
- Misuse of information technology systems
- General inaptitude
- General disciplinary causes—habitual or accumulated discrepancy causes

A security clearance is granted on your need to know and your meeting the standards for the level of clearance required. To get a security clearance, you must undergo a background investigation by an approved federal government agency. The higher the level of security clearance required, the more thorough the investigation. During the investigation, you are asked questions about your military, civilian, and personal conduct. You must answer the background questions completely and correctly.

Student Notes:

Just because you have a clearance doesn't automatically mean you have access to classified information. Having a clearance means you may be granted access if your duties require access to the information. This is called the *need to know*.

Security clearances and access to classified information are based on a *need to know*. Only Sailors who have a real need to know are cleared for access to the appropriate classified material. The command that has the classified material determines who has the need to know.

If you're cleared to work with classified material, censor what you say by keeping what you know to yourself. The following guidelines will help you safeguard classified material:

- Never reveal (talk about) classified information just to show your shipmates how smart you are or to act important. If they don't need to know the information to carry out their duties, don't tell them.
- Don't talk about classified information to unauthorized persons, including family, friends, shipmates, and especially strangers. Classified information can be unintentionally revealed to unauthorized persons in many ways.
- Interest in your own job is natural and desirable, but it must not lead you to reveal classified information to unauthorized persons. Never add to a news story that's incomplete, no matter how much you may know. If you do, you may make public what the Navy has tried to keep secret.

The SECNAV has designated the Department of the Navy Central Adjudication Facility (DON CAF) as the single clearance granting authority for the Department of the Navy. The DON CAF issues final security clearances for civilian and military personnel at the request of DON commands and activities once it has determined that granting the clearance is clearly consistent with the interests of national security. Once issued, a security clearance remains valid provided the Sailor continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months.

SECURITY AREAS

Classified information is always protected at the level of control appropriate with its assigned security classification level. This policy encompasses all classified information, regardless of media.

Personnel who work with classified information, work with it only in a secure facility. They use an accredited automated information system (AIS) under conditions that prevent unauthorized persons from gaining access to the material. If you have classified material in your possession, you are responsible for protecting that information. Lock classified material in an appropriate security container or facility when you're not using it or when it's not under your direct control.

If you work with classified material, you must follow procedures so unauthorized persons do not gain access to the classified information. In a facility that contains classified material, access is restricted and movement is controlled so personnel without a need to know do not have access to classified material. **All personnel must comply with the *need-to-know* policy**.

If you are using classified material, you can't remove it from the designated office or working area except to perform official duties and under conditions providing the protection required by SECNAVINST 5510.36.

Don't discuss classified material with any person that doesn't have a need to know.

STORING CLASSIFIED MATERIAL

The General Service Agency (GSA) sets 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 destruction of classified information.

When classified information isn't under the personal control or observation of a cleared person, it's guarded or stored in a locked GSA-approved security container or vault, modular vault, or secure room. For

Student Notes:

information about storage requirements, refer to SECNAVINST 1550.36.

MARKING CLASSIFIED MATERIAL

Classified material is marked so that personnel know the classified nature of the material, to make sure the material receives the degree of protection required, and to help extract, paraphrase, downgrade, and declassify the material.

All classified material is marked so you know the following information about the material:

- The level of classification
- The part(s) that contain(s) or reveal(s) classified information
- How long the material is to remain classified
- Additional measures needed to protect the material

Overall Markings

Material is marked so the security markings are easy to see and recognize. Classified documents are marked on their face and back cover and top and bottom center to show the highest overall classification level of the information they contain. (**NOTE**: Titles of classified documents are usually unclassified.) On documents, the classification level is marked or stamped in capital letters larger than the type used in the text to alert anyone handling the document that it is classified. Material is marked as follows:

AUTOMATED INFORMATION SYSTEM (AIS).—Removable AIS (fig. 22-1) storage media and devices used with AIS and word processors are marked using the appropriate SF label to indicate the highest overall classification level of information contained in the storage media.

PHOTOGRAPHS, SLIDES, AND TRANSPARENCIES.—The face of a classified photograph is marked with its highest overall classification level and associated markings. If this is not possible, these markings are placed on the back of the photograph. These markings are stamped or permanently affixed by pressure tape, labels, or other similar means.

Slides or transparencies (fig. 22-2) are marked with their highest overall classification level and association markings on the image area, border, holder, or frame. Groups of slides or transparencies used and stored together as a set are marked with their highest overall classification level and associated markings. Associated markings "Classified by," "Reason," "Derived from," and "Declassify on" are marked on the image area of the cover slide or transparency only.

MOTION PICTURE FILMS, VIDEOTAPES, AND CONTAINERS.—Classified motion picture films (fig. 22-3), videotapes, and their titles are prominently marked with the highest overall classification level and associated markings of the information they contain. The markings are visible when projected at the beginning and end of the production. Classified films, videotapes, and their containers are marked in the same manner.

SOUND RECORDINGS AND CONTAINERS.—Classified sound recordings (fig. 22-4) have an audible statement at the beginning and end of each recording. This statement identifies the highest overall classification level and associated markings of the recorded information. Containers of classified reels, cassettes, videotapes, and motion picture films are prominently marked with the highest overall classification level and associated markings of the information contained.

ROLLED OR FOLDED DOCUMENTS.—Rolled or folded blueprints, maps, charts, or other large items are clearly marked to show their highest overall classification level (fig. 22-5).

Portion Markings

Each portion such as the title, section, part, paragraph, or subparagraph of a classified document is marked to show its classification level. By doing this, a document is marked so you **know** what part or parts contain or reveal protected information. The classification level of a part of a document is shown by a classification symbol—TS for Top Secret, S for Secret, C for Confidential, and U for unclassified. The symbol

---

Student Notes:

Figure 22-1.—AIS storage media.

is placed in parentheses immediately following the part letter or numbers. If there aren't any part letters or numbers, place the abbreviation immediately before the beginning of the portion.

1. (U) This introductory sentence is Unclassified.

A. (C) This subparagraph is Confidential.

(1) (S) This subparagraph is Secret.

Examples of portion markings are shown in figure 22-6.

Student Notes:

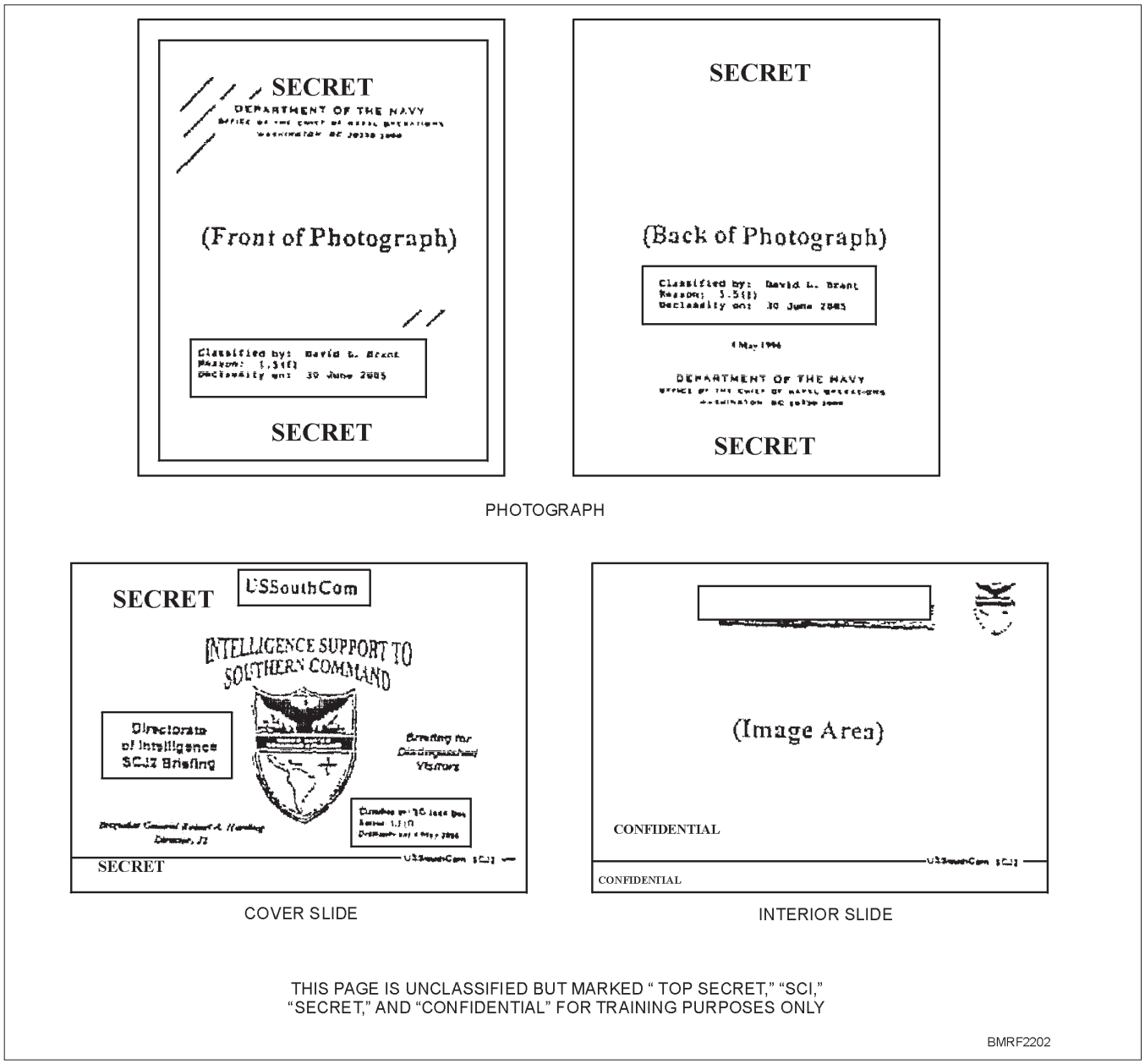


Figure 22-2.—Photographs, slides, and transparencies.

Marking Messages

Messages are marked in a manner similar to documents. They are marked with the highest overall classification level of the information contained in the message. Classified messages are marked to indicate the following:

- The nature of the classification—original or derivative
- The source of classification
- Downgrading instructions (if applicable)
- Declassification instructions (if applicable)

Student Notes:

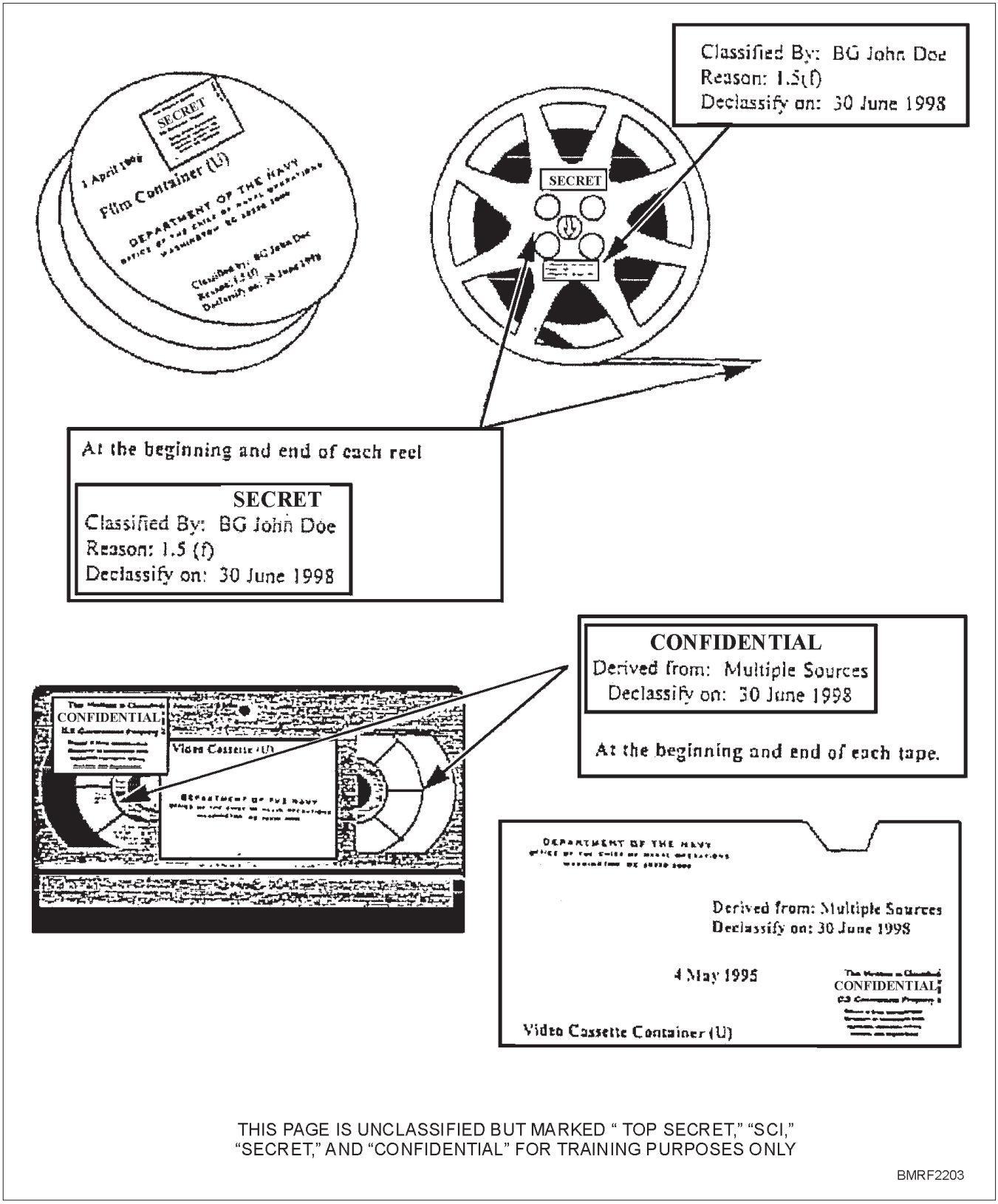
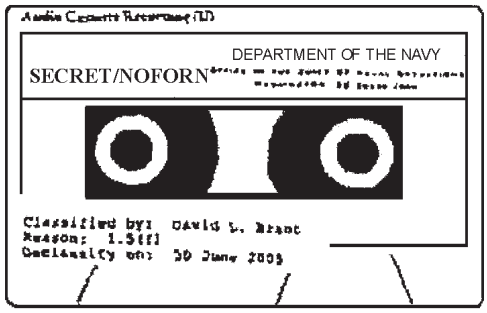
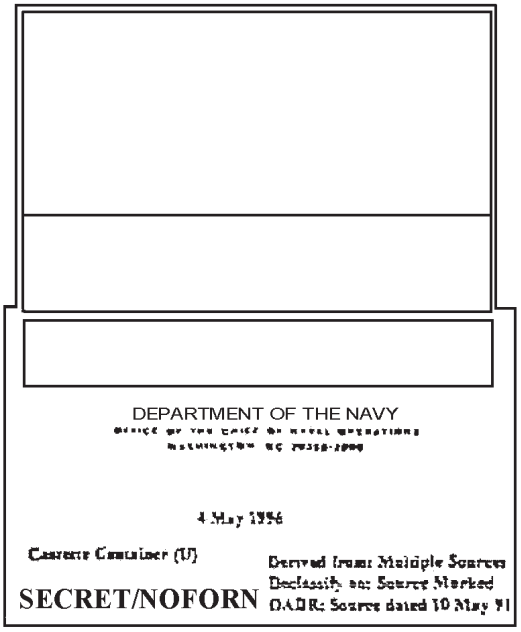
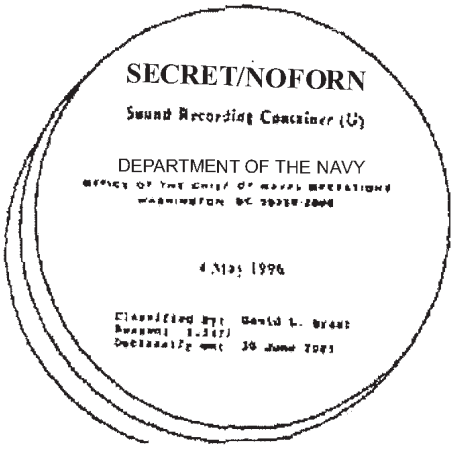


Figure 22-3.—Motion picture films, videotapes, and containers.

For more information on marking classified messages, refer to SECNAVINST 5510.36.







THIS PAGE IS UNCLASSIFIED BUT MARKED " TOP SECRET," "SCI,"
"SECRET," AND "CONFIDENTIAL" FOR TRAINING PURPOSES ONLY

BMRF2204

Figure 22-4.—Sound recordings and containers.

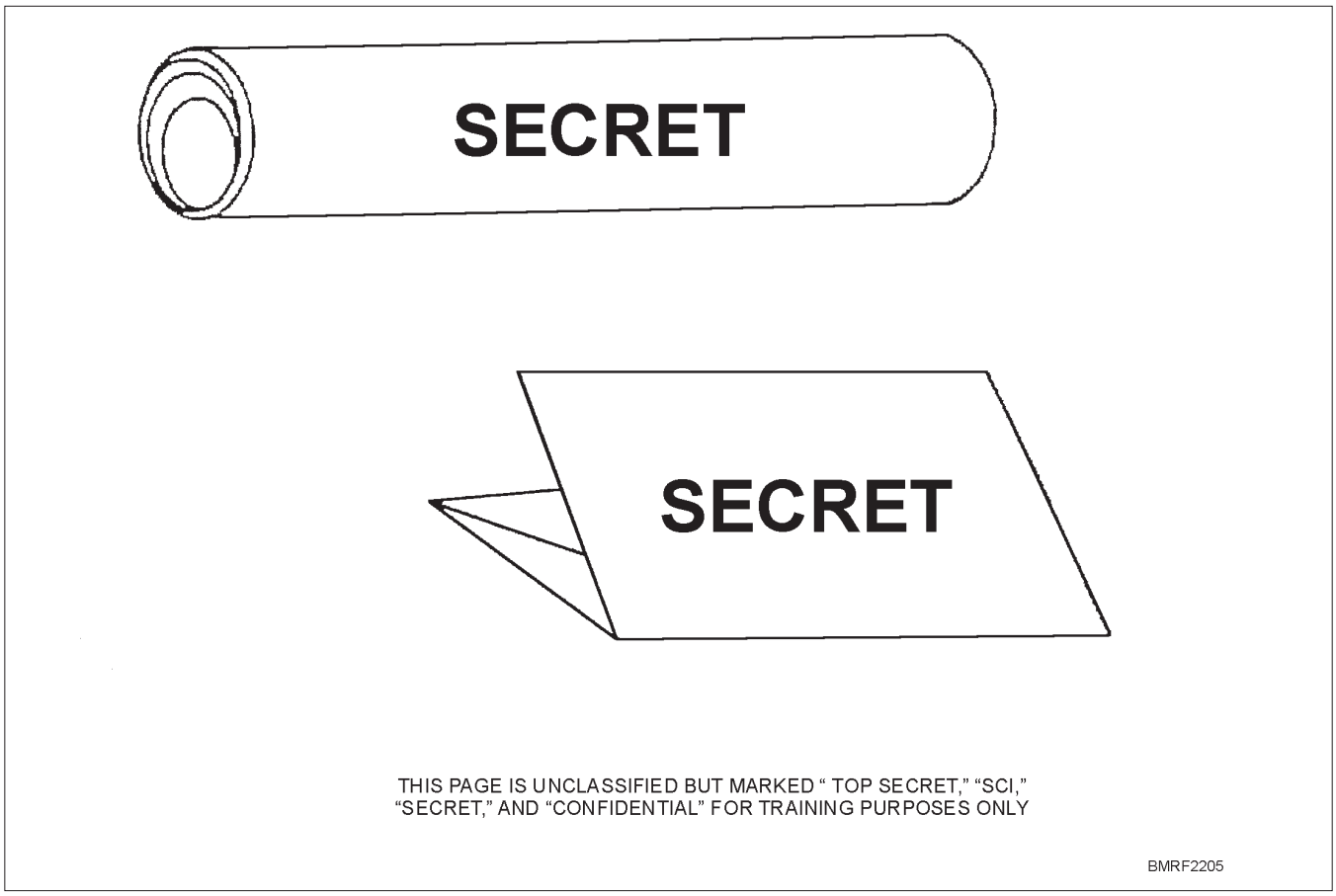


Figure 22-5.—Rolled or folded documents.

Miscellaneous Classified Material

Materials such as rejected copies, typewriter ribbons, carbons, and other similar items used during the production of a classified document are handled in a way that protects the material. Destroy such material when you no longer need it. You don't need to mark this material as classified unless it's necessary to ensure its protection.

TRANSMITTING CLASSIFIED MATERIAL

The rules for transmitting classified material can be found in the *Department of the Navy (DoN) Information Security Program*, SECNAVINST 5510.36. According to SECNAVINST 5510.36, commanding officers must make sure that only appropriately cleared personnel or carriers transmit, transport, escort, or hand-carry classified information. Unless a specific kind of transmission or transportation is restricted, the means selected should minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance.

Classified telephone conversations are permitted only over secure communication circuits. These circuits must be approved for the classification level of the information being discussed. Every attempt must be made to make sure that the classified information is not compromised to unauthorized personnel.

COPYING CLASSIFIED MATERIAL

U.S. classified information can be reproduced only to the extent required by operational necessity. However, the agency that originates the information may restrict reproduction of the material, or reproduction of the information may be restricted because of applicable statutes or directives.

Student Notes:

SECNAVINST 5510.36

OCT 16 1999

SECRET

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERRATIONS
Washington, DC 20350-2000

IN REPLY REFER TO

5510
Ser NO9N2/9C1234556
(Date)

SECRET—CONFIDENTIAL upon removal of enclosure (2)

From: Chief of Naval Operations
To: Director, Special Programs Office

Subj: CLASSIFIED LETTER OF TRANSMITTAL, TRANSMITTING A CLASSIFIED ENCLOSURE (U)

Encl: (1) CNO ltr 5510 Ser NO9N2/7U123445 of 12 Oct 96
(2) CNO ltr 5510 Ser No9N2/7S12345 of 28 Sep 96

1. (U) A classified letter of transmittal shall be marked as any other classified document with all applicable associated markings.

2. (C) This classified letter of transmittal contains Confidential information and has a Secret enclosure, therefore, its highest overall classification level is Secret, but Confidential when the Secret enclosure is removed. Instructions to this effect are annotated on the face of the letter of transmittal, top let corner, as shown.

3. (U) The declassification instructions, bottom left, reflect the disposition of the Confidential information contained in the classified letter of transmittal after the classified enclosure is removed.

John Boat
By direction

Derived from: OPNAVINST 5513.11B, enclosure (7)
Declassify on: Ccmpletion of test or 1 Jan 00

THIS PAGE IS UNCLASSIFIED BUT MARKED "TOP SECRET," "SCI," "SECRET," AND "CONFIDENTIAL" FOR TRAINING PURPOSES ONLY

SECRET

BMRf2206

Figure 22-6.—Portion markings.

DESTROYING CLASSIFIED MATERIALS

Classified material is destroyed in accordance with procedures contained in SECNAVINST 5510.36. Burn bags are used to store classified information awaiting destruction at a central destruction facility.

AUTOMATED DATA PROCESSING (ADP) SECURITY

Automated data processing (ADP) is a Navywide responsibility. It encompasses security aspects that contribute to the protection of the total ADP activity, office information system, or network. ADP security involves the following elements:

- Physical
- Administrative/operating procedures
- Hardware
- Software
- Data

Your command will have an automated data processing security officer (ADPSO) who reports to the CO on matters that concern the protection of electronically generated data. The ADPSO is responsible for the physical security of each computer workstation. The protection of each workstation involves physical security, physical access control, data file protection, and natural disaster protection. Seek out your ADPSO and make sure your workstation complies with Navy and command regulations for the protection of classified material.

Levels of ADP Security

Data processed electronically have three levels of security: Level I, Level II, and Level III. If your command processes Level I and/or Level II data, it must provide a specific degree of protection. The following chart defines the three levels of data:

LEVEL	MEANING
Level I	Classified data
Level II	Classified; requires special protection, such as For Official Use Only and data covered by the Privacy Act of 1974
Level III	All other unclassified data

Marking Removable Classified Automated Information System (AIS)

Pages or portions removed from AIS printouts (fig. 22-7) for separate use or maintenance are marked as individual documents. They are marked with the highest overall classification level and include all the required associated markings for all pages or portions that are removed.

Software used to produce classified material is programmed so that each classified file stored by the system is marked with the highest overall classification level and all associated markings. Also, the outside of AIS media storing classified files is programmed in a readily usable format with the highest overall classification level including all applicable warning notices and intelligence markings. AIS media that contains classified files not programmed in a readily accessible format are marked on the outside with the highest overall classification level and all applicable associated markings (normally a sticker or tag) or have marked documentation kept with the media.

The computer system and its associated peripherals require controlling and safeguarding at all times. This includes the disks, diskettes, disk drives, monitors, printer ribbons, and generated hard copy. Security procedures for electronic data is found in the *Department of the Navy ADP Security Manual*, OPNAVINST 5239.1.

Marking Disks

As a general rule, the two types of electronic media are the working copy media and finished media. Working copy media is temporary information. It stays in your work area and under the control of your activity. After creating a working copy, retain it for 180 days before destruction. Finished media is permanent information. It can be released to other commands and activities. Finished media contains information that doesn't change or is pertinent for more than 180 days.

Student Notes:

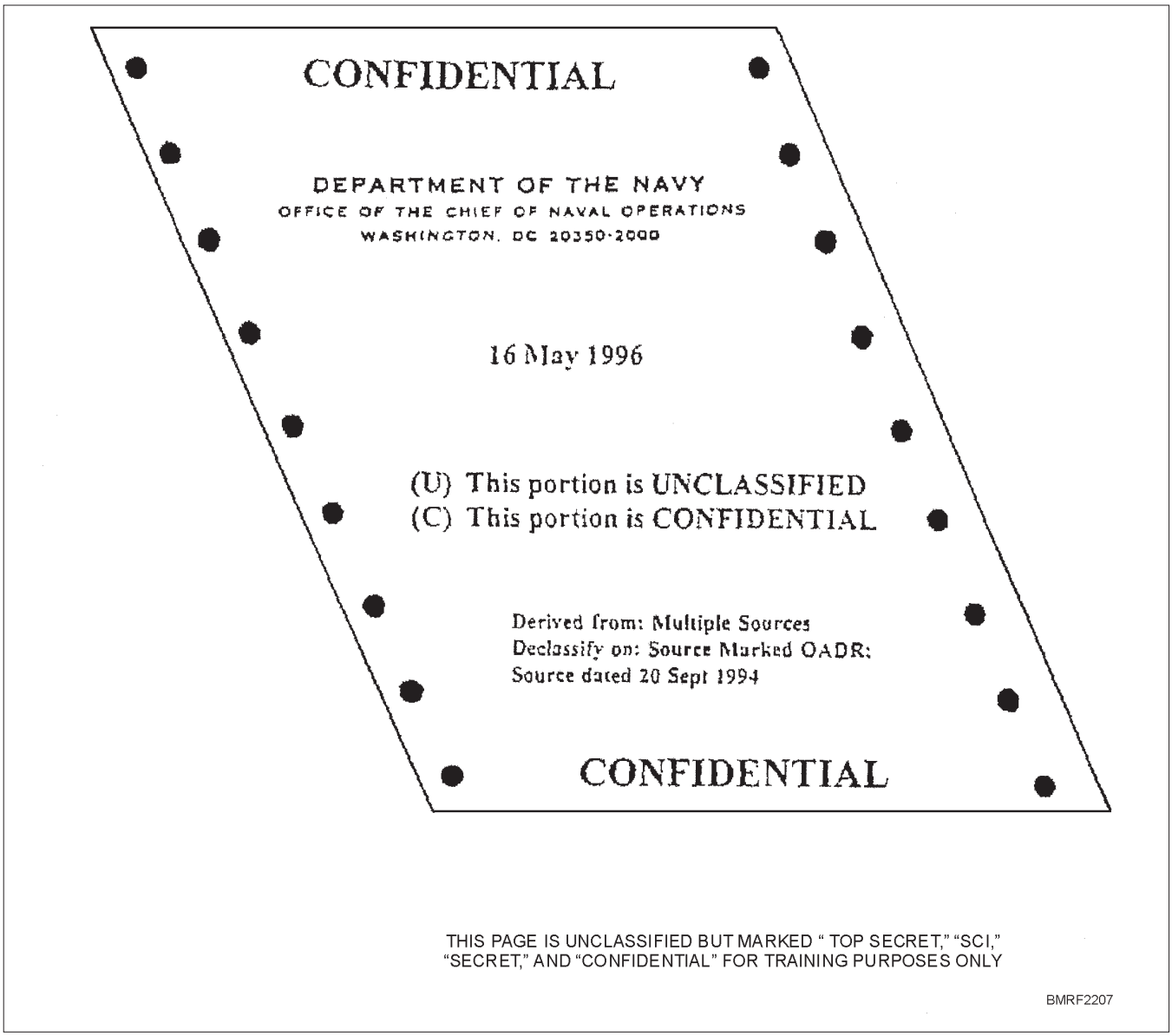


Figure 22-7.—Automated information system printout markings.

Electronic media is dated and the classification marked when it's created. Disks classified as Secret or Top Secret are assigned a sequential identification number so they can be tracked. Electronic media is controlled just like other classified material. Electronic media is protected according to the highest classification ever recorded on the disk.

Disks (see fig. 22-1) are marked with stick-on labels that identify the overall security classification and permanently assigned identification numbers.

The ADP security program protects ADP activities, office information systems, and networks. The management of the ADP security system is continuously monitored and reviewed for effectiveness. The *ADP Security Manual,* OPNAVINST 5239.1, contains a complete description of ADP security policies and procedures.

Student Notes:

COMPROMISE OF CLASSIFIED MATTER

According to SECNAVINST 5510.36, compromise is *An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance.* This means that material is compromised if someone loses, steals, captures, salvages, or sees the material without being cleared. The material is also compromised if a person who has seen the material defects.

The compromise of classified information threatens our national security. How much of a threat the compromise is depends on the nature and classification of the compromised material. If you know that material is compromised or subject to compromise, report the facts to your superiors right away. If you find classified documents where they don't belong, such as lying in the street or on a beach, turn the documents in to your superior or to the nearest military activity. While this doesn't seem possible, it has happened!

A security violation is defined as *any failure to comply with the regulations for the protection and security of classified material.*

If you find an unattended open or unlocked safe or container in which classified material is stowed, a security violation has been committed. You must report the discovery immediately to the senior duty officer. Then, guard the material until the duty officer arrives. After inspecting the material, the duty officer will lock the safe. If it's believed that the material is or may have been compromised, the duty officer will have the person responsible for the material make a detailed inventory.

PERSONAL CENSORSHIP

One form of classified material that can't be physically safeguarded is the information you carry around in your head. You are the only person who can prevent its disclosure. Be constantly on guard to prevent revealing classified information—either by talking or by writing.

A World War II slogan that's still effective is "Loose lips sink ships." Loose talk, even to a person who has the same knowledge you have, may be overheard by unauthorized persons. All of us like to talk about our ships, our jobs, and our travels. However, when we do, we should be sure we don't discuss classified information in our conversations.

Loose talk in public places can be especially damaging. Intelligence agents are trained to collect bits of seemingly harmless information. Putting all the bits together might produce a comprehensive file of classified information.

Never discuss classified information over telephones, as they constitute one of the least secure systems of communication. Telephones are subject to wiretapping—both physically and electronically. Long-distance circuits use microwave radio transmission, which is easily intercepted. The use of homemade or unauthorized codes, double-talk, or an attempt to talk around a classified subject provides no protection against trained intelligence personnel.

The methods used by foreign intelligence agents take many forms. An agent could be male or female, young or old, or of any national origin or background. Foreign agents exist in our everyday lives as ordinary people. They could blackmail you or make threats against you or members of your family. They may take the friendly approach and offer you friendship, money, or other things of value. They may even promise to assist your relatives living in a foreign country. They may offer any number of things in return for classified material or bits of information that seem unimportant to you. Always remember that people who deal in espionage are experts in dealing with people.

REPORTING SUBVERSIVE ACTIVITIES

Whether you have access to classified material or not, you must report to your commanding officer, through your chain of command, anyone you suspect is involved with espionage, sabotage, or is compromising classified material. If a stranger approaches you asking inappropriate questions when you are on leave or liberty status and you cannot contact your chain of command, report this information to the nearest military activity.

Being security conscious and following security standards and requirements is a big responsibility. However, maintaining proper security can be accomplished if you realize that security really is a personal concern.

Student Notes:

TERRORISM

Terrorism is the unlawful use or threatened use of force or violence against individuals or property. Terrorists intend to coerce (force) or intimidate governments or societies. Terrorism is used for political, religious, or ideological purposes. Acts of terrorism directed against naval personnel, activities, or installations can destroy critical facilities and injure or kill personnel. Terrorism can delay mission accomplishment and cause damage through adverse publicity and public perception (the way people see the action) of incident handling and results.

Terrorists use many methods of operation, which may include bombings, ambush, armed attack, sabotage, or taking hostages. The two most publicized terrorist methods are bombings and taking hostages. The terrorist method generally used toward military forces is bombing. However, at times, naval or military personnel have been taken hostage as a result of an aircraft highjacking or of highjacking personnel using some other means of transportation. Military personnel, and particularly naval personnel, are often stationed in or visit foreign countries. Some of these countries have significant levels of terrorist activity.

Indications and warnings of terrorist activity against naval installations or personnel are normally received from U.S. security authorities or through the security agencies of host countries. These warnings usually come in the form of threat conditions (THREATCONS). Threat conditions range from THREATCON ALPHA (the lowest degree of readiness) to THREATCON DELTA (the highest degree of readiness). Each threat condition contains several measures that must be adopted before that degree of readiness is fully set. When stationed in or visiting foreign countries, you will receive a brief concerning the threat condition in force at that time.

When visiting foreign countries, you must be constantly aware of what is going on around you. The actions of terrorist groups are rarely advertised. Terrorists normally choose places of business that have a high volume of target personnel present (such as nightclubs, restaurants, airports, and shopping centers). Be more careful at night, when the cover of darkness helps the terrorist hide his or her activities. Be alert and notice anything out of the ordinary and report it to the proper authorities. You could identify a possible terrorist operation.

Although terrorist attacks within the United States aren't as common as in other countries, they have happened. The same levels of awareness that you practice when visiting foreign countries are necessary here as well. Being alert when you are on or around military installations could mean the difference between the success or failure of a terrorist operation, not to mention the lives of your shipmates.

BOMB THREATS

When detonated or ignited, a bomb can injure or kill personnel and damage material. Bombs are classified as explosive or incendiary. An *explosive bomb* causes damage by fragmentation, heat, and blast. The heat produced often causes a secondary incendiary effect. An *incendiary bomb* generates fire-producing heat without substantial explosion when ignited. Bombing occurs when an explosive bomb detonates or an incendiary bomb ignites.

A bomb threat may happen anytime or anywhere. It can be made by a terrorist group or a disgruntled employee. Many bomb threats are unfounded (not real). False bomb threats make people complacent (at ease). Don't assume a bomb threat is a hoax (not real) until you're sure. **Safety is the major concern**!

Bomb threat. A bomb threat is a message delivered by telephone or letter. A bomb may be delivered through the mail as a letter or a suspicious package. A bomb threat may or may not contain the following information:

- The bomb's location
- The time for detonation/ignition
- An ultimatum related to the detonation/ignition or concealment of the bomb

Bomb incident. A bomb incident is the detonation/ignition of a bomb, discovery of a bomb, or receipt of a bomb threat.

Student Notes:

There are a few things you can do to reduce vulnerability of your ship or station to a bomb threat/incident. You can—

- Strictly comply with your command's procedures for personnel identification and access control procedures to department/division spaces,
- Be suspicious of all articles whose origin is unknown or obviously "out of place" within the space,
- Maintain tight control of locks and keys,
- Lock all rooms/spaces when not in use or manned by authorized personnel, and
- Immediately report suspicious personnel and their actions.

Each telephone at your command should have a copy of the Telephonic Threat Complaint, OPNAV Form 5527/8 (fig. 22-8). When a bomb threat is received by telephone, the person receiving the call should take the following actions:

- Try to keep the caller on the line and obtain as much information as possible. Complete the Telephonic Threat Complaint form while the caller is on the line or immediately thereafter.
- Record in writing the exact words of the caller.
- Try to identify the location of the bomb, the type of device, what it looks like, and the expected time of detonation.
- Attempt to determine the sex, approximate age, and attitude of the caller.
- Note any background sounds that may provide clues to the caller's location.
- Note any accent or peculiarity in speech that may help identify the person.

REVIEW 1 QUESTIONS

Q1. List the security classifications.

a.

b.

c.

Q2. What does FOUO stand for?

Q3. Who is authorized to initiate a request for a security clearance and background investigation?

Q4. A background investigation is required for what levels of security clearances?

Q5. What does a letter in parentheses, such as (S), after a publication title tell you about the publication?

Q6. How are classified material such as videotapes, cassettes, and computer disks marked?

Q7. A publication contains Confidential material, except for one paragraph that contains Top Secret material. How is this publication marked?

Student Notes:

DEPARTMENT OF THE NAVY

TELEPHONIC THREAT COMPLAINT

IF BOMB THREAT, ASK THE CALLER

- WHEN IS THE BOMB TO GO OFF?
- WHERE IS THE BOMB TO GO OFF?
- WHAT KIND OF BOMB IS IT?
- WHAT DOES THE BOMB LOOK LIKE?
- WHERE ARE YOU CALLING FROM?

1. COMMAND

a. Name & Address | b. Phone No

2. COMPLAINANT

a. Name

3. PERSON RECEIVING CALL

a. Name | b. Date & Place of Birth

c. Command Name & Address | d. Phone Number *(Work)* *(Home)*

4. TELEPHONE CALL RECEIVED ON

a. Phone Number *(Included area code)* | b. Location

c. Phone Number listed in *("x" all that apply)* ☐ Command Directory ☐ Base Directory ☐ Local Directory ☐ Unlisted ☐ Other *(list)*

5. DETAILS OF CALL

a. Date | b. Day of Week | c. Time

6. CONTEXT OF CONVERSATION

a. Recipient

b. Caller

c. Recipient

d. Caller

e. Recipient

f. Caller

7. BACKGROUND NOISES *(Describe street sounds, voices, music, etc.. If more space is needed, continue on reverse.)*

8. INFORMATION ABOUT CALLER/VOICE CHARACTERISTICS

a. Sex | b. Age | c. Race | d. Accent

e. Educational Level | f. Attitude *(Calm, Nervous, Serious)*

g. Other

9. WERE THERE ANY WITNESSES TO THE CALL? ☐ No ☐ Yes *(List name)*

10. DO YOU HAVE ANY SUSPICION AS TO THE IDENTITY OF THE CALLER? ☐ No ☐ Yes *(List name)*

11. NOTIFICATION OF AUTHORITY *("x" all notified)*

☐ CO ☐ XO ☐ OOD ☐ Security ☐ NISRA ☐ Telephone Company ☐ EOD ☐ Fire Dept

OPNAV 5527/8 (12-82) S/N 0107-LF-055-2740 BMRf2208

Figure 22-8.—Telephonic Threat Complaint, OPNAV Form 5527/8.

Q8. What type of area is used to keep classified material?

Q9. What type of material is safeguarded through ADP Security?

Q10. You are making your rounds as a roving security patrol and discover that the door to the radio room is unlocked and the room unattended. What action should you take?

Q11. The least secure system of communication should never be used to discuss classified material. What is the least secure communications means and why should it never be used to discuss classified material?

Q12. You are on leave away from your command. You meet someone who starts asking questions about your command and its mission. What should you do?

Q13. What are the two most publicized methods of terrorism?

a.

b.

Q14. Where is the likely spot for a terrorist bombing to occur?

Q15. What form is used to record bomb threats received over the phone?

Q16. If you receive a bomb threat over the phone, what should you do?

INTERNATIONAL AGREEMENTS

Learning Objectives: When you finish this chapter, you will be able to—

- Identify the purpose of international agreements.
- Recall the general provisions of the Status of Forces Agreement, the Geneva Convention concerning treatment and rights of prisoners of war, and the Law of Armed Conflict.

Many agreements are made between the government of the United States and governments of other countries. Some of the agreements that directly affect you are discussed in this chapter. These international agreements are the Status of Forces Agreement (SOFA), the Geneva Convention, and the Law of Armed Conflict.

During your tour of duty in the Navy, you will have the opportunity to visit other countries. You may visit as a member of a ship's company, or you may be assigned to a duty station overseas. In either case, remember that you are a guest of the country you are visiting. A small percentage of people feel because they are members of the U.S. Navy, local laws don't apply to them. **That is not true**. If you are on leave or liberty in a foreign country, you must obey the laws of that country.

STATUS OF FORCES AGREEMENT

It is the policy of the Department of Defense (DOD) to protect your rights as much as possible if you are subjected to criminal trial by foreign courts. To do that, the United States has entered into an agreement with several of our allied countries. That agreement is called the *Status of Forces Agreement* (*SOFA*). The SOFA says, in part, that the host country will give up some of

Student Notes:

its jurisdiction to the visiting country in some criminal and civil cases. **The main purpose of the SOFA is to clearly define the status of military personnel of one country stationed in the territory of another**. Some of the topics covered by the Status of Forces Agreement are as follows:

- Freedom of troop movement within the host country
- Passport requirements
- Criminal jurisdiction
- Taxes
- Imposition of customs duties
- Regulations covering driver's licenses

These are just a few of the items covered by the SOFA. (Provisions of the SOFA vary from country to country.) Remember, when you are overseas, YOU are the foreigner. Many customs of the host country may seem strange to you, but you must follow them as well as the local laws. You should receive a briefing on the Status of Forces Agreement that pertains to the country you are visiting. If you have any questions concerning the SOFA while you are in a foreign country, consult your division officer.

GENEVA CONVENTION

Prisoners of war (POWs) have certain rights and are required to observe certain rules, as established by the Geneva Prisoners of War Convention of 1949. The Geneva Convention prescribes the following rights of POWs:

- To be treated humanely at all times
- To be protected against insults and public curiosity
- To have decent housing, nourishing food, and adequate clothing
- To be permitted to communicate with their families
- To be given medical care
- To be allowed to worship
- To be allowed to excerise and participate in sports and intellectual pastimes

The Geneva Convention prohibits punishment for refusing to answer questions other than your name, date of birth, rate, and social security number.

A prisoner must salute enemy officers and may be required to perform work if such work is not related to military operations. POWs are subject to the laws, regulations, and orders of the armed forces of the captors and may be punished for violating them. The Geneva Convention recognizes the prisoner's right to try to escape by limiting punishment for such attempts to disciplinary action only, which may consist of 2 hours extra duty daily, loss of half a month's pay (earned as a prisoner), stoppage of any extra privileges, and confinement. A prisoner may not be punished more severely for repeated escape attempts. Prisoners of war are prohibited from renouncing any of the rights to which they are entitled under the Geneva Convention.

Most countries of the world follow the articles of the Geneva Convention. North Vietnam agreed to the convention in 1957 but violated most of its provisions. In 1965, Hanoi violated the convention by announcing the execution of three American POWs in retaliation for the legal execution of Viet Cong terrorists. The Communists also paraded handcuffed Americans through the streets of Hanoi where the people subjected them to ridicule and humiliation. The Geneva Convention expressly forbids such actions. Evidence also indicates that Iraq violated some articles of the convention during the Persian Gulf crisis.

If you have contact with enemy prisoners of war, treat them according to the articles of the Geneva Convention, just as you would expect to be treated by them. If you should become a POW, you should conduct yourself according to the Code of Conduct as well as the Geneva Convention.

LAW OF ARMED CONFLICT

Every nation calls upon its military personnel to defend its national interests by going to war. Our country believes those people involved in armed conflict during war are entitled to fundamental human

Student Notes:

rights regardless of their conduct or beliefs. Because of this belief, our nation has adopted the Law of Armed Conflict to govern the conduct of its military forces engaged in fighting.

Because naval operations frequently involve fighting between major units, you don't need a detailed knowledge of the Law of Armed Conflict. However, you need a basic knowledge of it since even in large-scale naval operations some people may violate the Law of Armed Conflict.

Small-scale operations require a more detailed knowledge of the Law of Armed Conflict by the naval personnel involved. You will receive this detailed knowledge if the need arises.

As a member of a military force, you are allowed during periods of hostilities to attack and even kill the lawful combatants of your enemy. Generally speaking, the term *lawful combatants* means members of the military force and civilian personnel engaged in hostilities.

Just as the Law of Armed Conflict permits certain hostile actions, it limits the way you may conduct these actions. It provides for the protection of certain targets in a war zone to safeguard people and property not directly involved with military activity. For example, it expressly forbids attacking or firing on nonmilitary targets not being used by the enemy for military purposes. The use of illegal techniques and tactics, such as rape, pillage, and plunder, is also prohibited. Unlawful techniques and tactics can backfire on the user because often they are dangerous in themselves. They are also likely to enrage the enemy, causing the enemy to fight harder or respond by using illegal methods, such as killing POWs. Personnel who violate the Law of Armed Conflict will find themselves in serious trouble, including the possibility of trial by court-martial upon return to the United States.

The fundamental terms of the Law of Armed Conflict are as follows:

- Fight only enemy combatants.
- Destroy no more than your mission requires.
- Do not attack enemy soldiers, sailors, airmen, or marines that surrender. Disarm them and turn them over to your superior.
- Never torture or kill prisoners of war and other detainees.
- Collect and care for wounded, sick, or shipwrecked survivors, whether friend or enemy, on land or at sea.
- Protect medical personnel and chaplains, medical and religious facilities, and medical transportation of the enemy. Treat them with respect and do not attack them.
- Treat all civilians humanely and respect their property. Do not attack them.
- Do your best to prevent any violation of these fundamental rules. Report any violations to the appropriate authority promptly.
- Do not violate these rules; an order to do so is illegal.

Discipline yourself to obey these rules during combat. Disobedience of the Law of Armed Conflict dishonors your nation, the Navy, and you. Far from weakening the enemy's will to fight, such disobedience strengthens it. Disobedience of the Law of Armed Conflict is also a crime punishable under the *Uniform Code of Military Justice.*

REVIEW 2 QUESTIONS

Q1. What is the main purpose of the SOFA?

Q2. What document dictates the treatment of POWs?

Q3. What is the purpose of the Law of Armed Conflict?

Student Notes:

SUMMARY

Security of classified material is serious business. Potential enemies are always looking for a chance to gain access to our most guarded secrets. Just one day of failing to safeguard classified material could result in the compromise of extremely sensitive material. The security of classified material not only rests with the personnel that have access to it on a daily basis, but also includes every member of a command. We all have a duty to ensure that only the people requiring access to classified material are allowed to see or use it. The same is true of how we discuss our daily routine. Even if you don't have access to classified material on a daily basis, you could possibly have knowledge of certain exercises or deployment times that world be of benefit to potential enemies. Think carefully before you start talking about upcoming events. Every person in the room is not cleared to have this type of information. Putting pieces of information together to determine what is happening is easy for foreign agents. The same is true when talking on the telephone. Very few phones aboard ship and almost none in the civilian community are secure. Electronic eavesdropping is another way foreign agents collect intelligence data. Be careful of what you say; someone other than the person you called could be listening.

Terrorist activity, particularly when you are visiting a foreign country, should always be of concern. While you should not let it interfere with your enjoyment of visiting a foreign country, you must always be alert to what is going on around you. By taking an extra few minutes to survey your surroundings, you could identify a potentially hazardous situation.

The international agreements discussed were designed to protect members of the armed forces. The Status of Forces Agreement protects you when you are stationed in or visiting foreign countries. The Geneva Convention affords you protection if you become a POW. The Law of Armed Conflict protects you in the event of a war. The articles and rules of these agreements will only protect you if you conduct yourself according to U.S. and international law. You have a duty to conduct yourself in a manner that will not bring discredit upon your country, your service, or yourself.

REVIEW 1 ANSWERS

A1. The three levels of security are—

a. **Top Secret**

b. **Secret**

c. **Confidential**

A2. FOUO means **For Official Use Only**.

A3. **Commanding officers** are authorized to initiate a request for a security clearance and background investigation.

A4. A background investigation is required for **Top Secret** and **Secret** clearances.

A5. A letter in parentheses, such as (S), after a publication title tells you **the classification of that publication.**

A6. Classified material, such as videotapes, cassettes, and computer disks, are **marked by tags, stickers, decals, and so on.**

A7. Publications carry the security marking of the highest level of material contained in the publication; therefore, **this publication is marked Top Secret**.

A8. **Security areas** are used to keep classified material.

A9. ADP security is used to safeguard **data processing equipment (computers) including hardware, software, administrative and operating procedures, communications, and personnel and spaces**.

A10. If you find an unattended room with an open and unlocked security container, you should **contact the senior duty officer to report a security violation.** Then, **stand guard over the space until the duty officer arrives**.

A11. The least secure communications means is the **telephone**. **Never use telephones to discuss classified material because they can be physically and electronically wiretapped.**

Student Notes:

A12. If you meet someone who starts asking questions about your command and its mission, you should **report the incident to the nearest military activity**.

A13. The two most publicized forms of terrorism are—

a. **Taking hostages**

b. **Bombing**

A14. Terrorists are likely to bomb **places of business that serve a high volume of people such as airports, nightclubs, and restaurants**.

A15. To report a bomb threat made over the telephone, use **Telephonic Threat Complaint, OPNAV Form 5527/8**.

A16. If you receive a bomb threat over the phone, you should—

a. **Keep the caller on the line and get as much information as possible**.

b. **Record in writing the caller's conversation**.

c. **Ask caller where's the bomb, what type of bomb, time of detonation, and what it looks like**.

d. **Try to determine sex, age, attitude of caller, and accents or speech impediments; try to remember background noises**.

REVIEW 2 ANSWERS

A1. The main purpose of the SOFA is t**o define the status of military personnel of one country stationed in a territory of another**.

A2. The treatment of POWs is covered by the **Geneva Convention**.

A3. The purpose of the Law of Armed Conflict is **to govern the conduct of military personnel engaged in fighting**.

CHAPTER COMPREHENSIVE TEST

1. How many security classifications does the Navy use to identify classified material?
    1. One
    2. Two
    3. Three
    4. Four
2. Which of the following security classifications is used for information or material that requires the highest degree of protection?
    1. Top Secret
    2. Secret
    3. Confidential
    4. For Official Use Only
3. Having a security clearance automatically grants you access to classified material.
    1. True
    2. False
4. To get a security clearance, you must be a United States citizen.
    1. True
    2. False
5. Which of the following infractions will cause a Sailor's CO to report that infraction to DON CAF?
    1. Criminal conduct
    2. General inaptitude
    3. Noncompliance with security requirements
    4. All of the above
6. Classified material is assigned a security classification for which of the following reasons?
    1. To ensure personnel are aware of the classified nature of the material
    2. To ensure the material receives the degree of protection required
    3. To assist in extracting, paraphrasing, downgrading, and declassifying actions
    4. All of the above
7. If a publication contains unclassified, FOUO, Confidential, Secret, and Top Secret information, what security classification is assigned?
    1. Top Secret
    2. Secret
    3. Confidential
    4. For Official Use Only
8. If you need to find the rules for transmitting classified material, you should refer to what SECNAV instruction?
    1. 5510.36
    2. 5510.30A
    3. 5510.3
    4. 5510.3A
9. Classified information is not transmitted over the telephone except when authorized on approved, secure communications circuits.
    1. True
    2. False
10. Which of the following is a concern of ADP security?
    1. Hardware
    2. Software
    3. Admin procedures
    4. All of the above
11. What term defines classified material that is lost, stolen, captured, salvaged, or seen by unauthorized personnel?
    1. Secure
    2. Abandoned
    3. Compromised
12. What type of communications is one of the least secure communications system?
    1. Registered U.S. mail
    2. Telephone
    3. U.S. mail
    4. Courier Service

13. What action, if any, should you take if you suspect someone you know is compromising classified material?

    1. Confront the individual
    2. Report it to the command security officer
    3. Report it to your CO through the chain of command
    4. None

14. Terrorists try to force governments or societies to take certain actions for political, religious, or ideological purposes.

    1. True
    2. False

15. The greatest publicity is given to which of the following terrorism methods?

    1. Taking hostages
    2. Bombing
    3. Both 1 and 2 above
    4. Sabotage

16. Which of the following threat conditions affords the highest degree of readiness?

    1. ALPHA
    2. BRAVO
    3. CHARLIE
    4. DELTA

17. The Status of Forces Agreement covers which of the following topics?

    1. Taxes
    2. Criminal jurisdiction
    3. Passport requirements
    4. All of the above

18. In what year did the Geneva Prisoners of War Convention establish certain rights for prisoners of war?

    1. 1948
    2. 1949
    3. 1950
    4. 1951

19. The Law of Armed Conflict prohibits which of the following techniques or tactics?

    1. Rape
    2. Pillage
    3. Plunder
    4. All of the above

20. The Geneva Convention recognizes a prisoner's right to try to escape. Which of the following disciplinary actions may be taken when a prisoner is caught in an escape attempt?

    1. Stoppage of extra privileges
    2. Confinement
    3. Both 1 and 2 above
    4. Torture