CHAPTER 3

SAFETY AND SECURITY

SAFETY

RESPONSIBILITY

Responsibility for the safety of personnel is vested in the commanding officer. Article 0732 of the U.S. Navy Regulations reads as follows:

> "The commanding officer shall require that persons concerned are instructed and drilled in all applicable safety precautions and procedures, that these are complied with, and that applicable safety precautions, or extracts therefrom, are posted in appropriate places. In any instance where safety precautions have not been issued or are incomplete, he shall issue or augment such safety precautions as he deems necessary, notifying, when appropriate, higher authorities concerned."

While commanding officers cannot delegate this responsibility for the safety of all personnel under their command, they must necessarily delegate sufficient authority to all officers and petty officers under their command to ensure that all prescribed safety precautions are understood and enforced according to U.S. Navy Regulations.

Safety References

Personnel safety is a major responsibility of every electronics material officer (EMO). Electronic equipment enforces a stern safety code and violators are likely to be electrocuted on the spot. Because of the dangers inherent in working with electronic equipment, safety precautions should be made an important part of any training program. Basic electronic safety procedures are given in the following publications:

1. *Electronics Installation and Maintenance Book (EIMB) General,* Section 3, NAVSEA 0967-LP-000-0100

2. *Safety Precautions for Forces Afloat,* OPNAV 5100.19

3. *Standard Organization and Regulations of the U.S. Navy,* chapter 7, OPNAVINST 3120.32 series

4. Electronics Information Bulletin (EIB), NAVSEA 50111-80-EIB-XXX Stock #0967-LP-001-3XXX

5. Fathom (Surface Ship and Submarine Safety Review)

6. Lifeline (the Navy Safety Journal)

7. Ship's Safety Bulletin (NAVSAFECEN)

8. *Naval Ships Technical Manual* (NSTM), chapter 300

9. *Electric Shock, Its causes and Prevention,* NAVSEA 0900-LP-007-9010

10. *Technical Manual for Radio Frequency Hazards,* NAVSEA 0900-LP-005-8000

The EMO's responsibilities concerning safety generally encompass the areas of safety education, safety promotion, and safety enforcement.

Most electric shocks are due to human failure rather than equipment failure. However, equipment may suddenly fail and cause fatal shock even though carefully designed for safety, thoroughly tested before use, and used in accordance with applicable safety precautions.

Nearly all shipboard deaths are caused by human failure manifested in one or more of the following ways:

Unauthorized use of, or unauthorized modifications to, equipment.

Failure to observe the applicable safety precautions when using equipment or when working on or near energized equipment.

Failure to repair equipment which was known to be defective and had previously given a mild shock to users.

Failure to test and inspect equipment for defects or failure to remedy all defects found by tests and inspections.

All of these failures may be summarized as failure to observe applicable safety precautions.

SAFETY EDUCATION

Personnel often will not observe safety precautions unless they are fully aware of the dangers involved in not observing them. The EMO's first duty, therefore, is to ensure that all personnel in the division are aware of the dangers and the safety precautions necessary to combat these dangers.

Safety precautions are dependent to some extent upon the type of ship involved. Precautions that must be strictly observed on ships such as AOs and AEs, may not apply to other types of ships. Nuclear powered ships have safety precautions which differ markedly in specific, important ways. Each ship or group of ships of the Navy is unique and will have special safety precautions to be observed. Type commanders require that the electronics doctrine (in the Division Organization Manual) have a safety section. Thus, personnel must read and understand all safety precautions pertaining to their own ship's equipment.

Safety precautions written for personnel in all ratings should include information concerning electric shock, and precautions to be observed when using electrical and electronic equipment aboard ship. Facts to be brought out and points to be stressed concerning electric shock should include the following general warnings:

1. Voltages as low as 30 volts can be fatal.
2. The dangers from electric shock are much greater aboard ship than ashore.
3. There is very little difference between a slight tingle and a fatal shock.

Current flow through the body is the cause of electric shock. Factors determining the extent of body damage due to electric shock are the amount and duration of the current flow; the parts of the body involved; and, in the case of a.c., the frequency of the current. In general, the greater the current or the longer the current flows, the greater will be the body damage. Body damage is likely when the current flow is through or near nerve centers and vital organs. An alternating current frequency of 60 hertz is considered slightly more dangerous than current of a lower frequency or than direct current. This is because ventricular fibrillation is produced with just a 60-100 mA current at 110-220 V a.c., 60 hertz while at d.c. voltage, 300-500 mA is required for the same reaction. However, the same precautions that apply to 60-hertz a.c. also apply to d.c.

Humans differ in their resistance to electric shock, and, consequently, a current flow that may cause only a painful shock to one person might be fatal to another. Table 3-1 presents information on the effects of 60-hertz current flowing through the body from hand to hand or foot to foot.

Tests made by the Bureau of Standards show that the resistance of the human body may be as low as 300 ohms under unfavorable conditions

Table 3-1.—Effects of 60-Hertz Value on Human Beings

Current Value	Effects
Less than 1 mA	No sensation
1 to 20 mA	Mild sensation to painful shock; may lose control of adjacent muscles between 10 and 20 mA.
20 to 50 mA	Painful shock with probable loss of control of adjacent muscles.
100 to 200 mA	May cause a heart condition known as ventricular fibrillation, which results in almost immediate death.
Over 200 mA	Severe burns and muscular contractions so severe that the chest muscles clamp the heart and stop it for the duration of the shock.

(such as those caused by salt water and perspiration). This indicates that it is possible for a potential difference as low as 30 volts to cause the fatal 100 milliampere current flow through the body. This leaves no doubt as to the danger involved and precautions necessary regarding the electrical circuits aboard ship.

The safety instructions to personnel in nonelectrical ratings should emphasize the following points about portable electrical equipment:

1. Always visually inspect portable electrical equipment before using. Look for damaged plugs, frayed cords, broken or missing ground connections, and the like.

2. Never use portable electrical equipment if there is reason to believe it might be defective. Have it tested by authorized personnel.

3. Make no repairs.

4. Do not use any personal portable electrical equipment aboard ship unless it has been inspected and approved by the ship's electrical shop or electronics shop according to ship's instructions.

5. Always report any shock received from electrical equipment, regardless of how slight.

PROMOTING SAFETY

Promoting safety within the division, or on the ship in general, will require that all hands become safety conscious to the point that they automatically consider safety in every job or operation. Through the use of safety reminders and by the example set by technicians, this safety consciousness will pass from one crew member to another.

All personnel, even the "old hands," need to be reminded occasionally to work safely. The senior electrical and electronics rates involved in fatal accidents bear out this fact.

Signs and Posters

Promoting safety within the division can be done in various ways. Posters are helpful as safety reminders and in promoting safety. Electrical safety posters are listed in the EIMB, *General Handbook* (NAVSEA 0967-LP-000-0100) and in NAVSUP 2002. Safety posters should be changed or rotated regularly to different working areas so as to draw attention to them. Posters put up and left in one area for months become part of the bulkhead and are ignored, written on, or covered with notices, schedules, or plans of the day. Warning signs are also listed in the same EIMB and should be part of every EMO's safety program.

Safety Patrols

Periodic safety patrols or inspections made by the Safety Petty Officer in the division can also be helpful in promoting safety within the group. This procedure is helpful in two ways. First, it establishes control of the safety program, and second, it makes the inspectors, who are members of the technician group, mindful of the

procedures necessary to ensure personnel safety. Standard Organization and Regulations of the U.S. Navy, OPNAVINST 3120.32 series, Chapter 7 outlines the duties of the Safety Petty Officer.

Safety Discussions

In addition, occasional short group training discussions concerning electrical safety are recommended. These discussions may take place at any time without prior preparation. There may be one person in the group, who has received a slight shock. This experience can be the basis of the discussion. The person concerned should relate the exact circumstance under which the shock was received. The group then can discuss the slightly different conditions that might have prevailed under which the shock could have been more severe or perhaps fatal. The discussion may then be directed toward a remedy for the condition causing this shock. If necessary, the appropriate action should be taken to eliminate the possibility of future shocks from this source.

ENFORCING SAFETY

Safety is no accident. EMOs will do well to be guided by the underlying principle that accidents can be avoided only in advance.

Many accident producing circumstances have already been recognized and anticipated in equipment instruction books, various safety manuals, and the ship's organization and regulation manual. In totality they represent a program broadly based on safety precautions and safety regulations. Precautions basic to a safety program may include the appropriate positioning of safety equipment, posting of warning signs, and the scheduling of safety discussions and demonstrations. These measures are all directed at promoting awareness and favorably affecting attitude. Safety regulations, on the other hand, are enforceable precautionary measures designed to ensure the safety of the ship and its personnel during a specific activity. The goal of personnel safety is to keep personnel safe from injury or death.

Safety Organization

In order to coordinate the overall shipboard effort in monitoring and evaluating the safety program without relieving any person in the chain of command of his assigned responsibilities, a safety organization will be established.

Figure 3-1 is an example taken from OPNAVINST 3120.32 series. The organization, under the supervision of the safety officer, shall accomplish the following:

1. Monitor accident prevention standards
2. Evaluate the effectiveness of the safety program
3. Coordinate distribution of safety information
4. Coordinate shipboard training in general accident prevention
5. Monitor submission of accident/injury/safety reports
6. Analyze accident and injury data to determine trends and ensure the effectiveness of corrective action
7. Detect and report safety hazards and violations
8. Monitor corrective action on safety items
9. Maintain liaison with outside commands in matters of accident prevention
10. Monitor and coordinate vehicular safety training
11. Monitor and coordinate recreational safety training

DIVISION SAFETY OFFICER.—The EMO/division officer will be the safety officer for his division. He shall:

1. Keep department safety officer advised on the status of the unit's safety program within the division

2. Act as divisional point of contact in coordinating and evaluating the unit safety program

3. Designate a senior petty officer, E-6 or above if available, as division safety petty officer

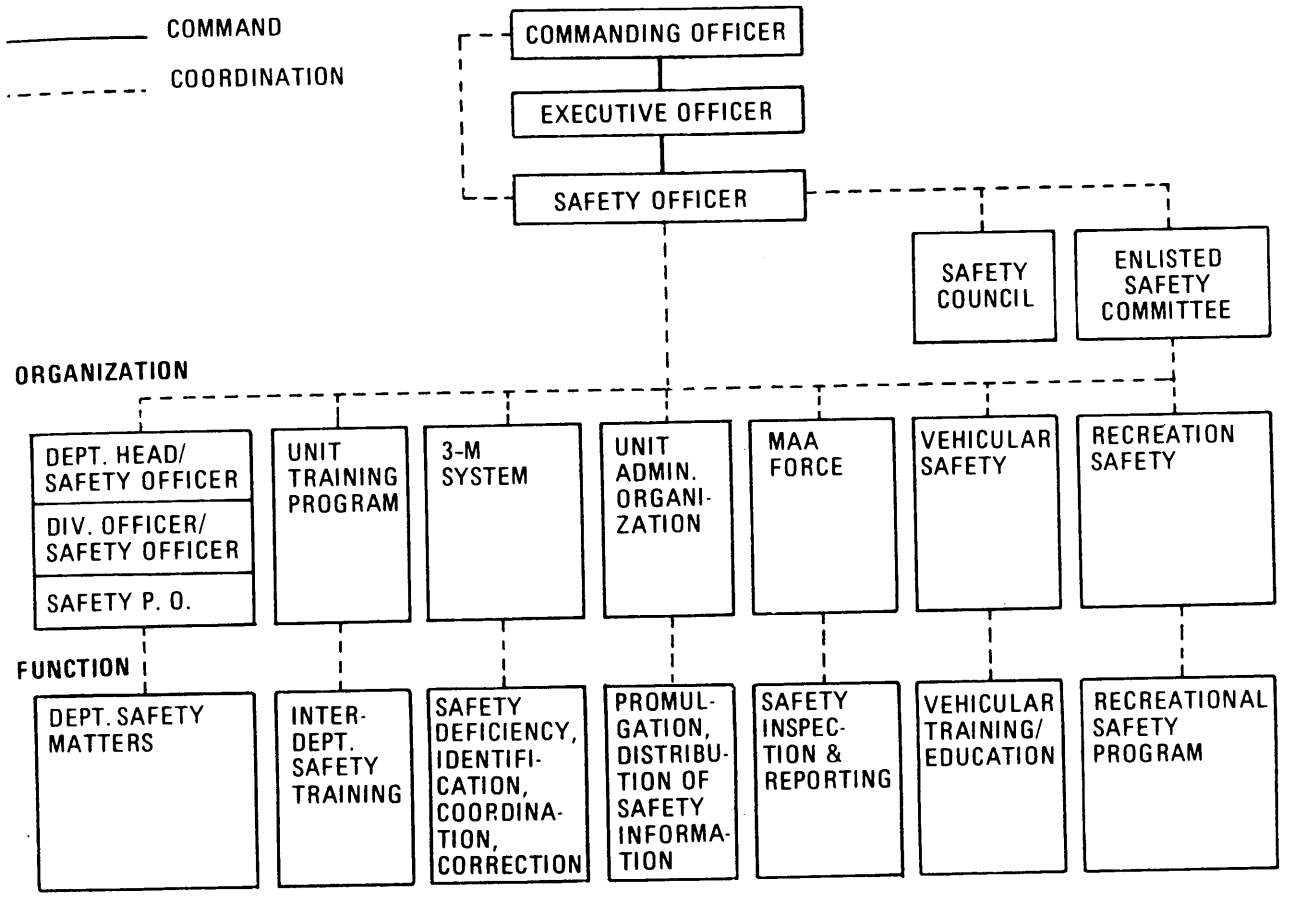


Figure 3-1.—Typical Safety Organization.

4. Investigate divisional accidents and near accidents

5. Ensure that corrective action is taken immediately on hazardous situations revealed by accident and hazard reports and on recommendations made in accident/injury reports

6. Ensure that divisional personnel receive accident prevention training

DIVISION SAFETY PETTY OFFICER.—The division safety petty officer will:

1. Become thoroughly familiar with all safety directives and precautions concerning his division

2. Conduct assigned divisional accident prevention training, and maintain appropriate records

3. Assist in investigations as directed

4. Make recommendations concerning the safety program to the division officer

5. Assist the division officer in the execution of safety duties

6. Act as a technical advisor on matters of accident prevention within the division

7. Serve on the safety committee

Figure 3-2 is a representative format for an internal reporting system. The procedures to be

MAA/SAFETY FORCE SECTION

Issued by:		To:	
Date:	Time noted:	☐ Urgent ☐ Priority ☐ Routine	
Location of Hazard:			
Nature of Hazard:			

DIVISION OFFICER SECTION

Corrective Action Taken:	
Recommended Additional Action by Seniors:	
Date forwarded:	Signature:

DEPARTMENT HEAD SECTION

☐ Above Action Adequate, or	☐ Additional Action Taken/Required as Follows:
Date Forwarded:	Signature:

	Initials	Date	Comments:
Safety Officer			
Executive Officer			
Commanding Officer			OPNAV Form 5102/or 5102/2 required ☐ Yes ☐ No

INSTRUCTIONS

This form (to be reproduced locally) is to be issued by any member of the safety force and delivered to the division officer concerned. Deliver duplicate copy to the safety officer. Division officer forward with action taken/recommended within one working day. Use reverse side if additional space is required for any section.

Figure 3-2.—Safety Hazard Report.

followed before working aloft will assist you in your safety program.

Working Aloft

The communications watch officer, combat information center watch officer, duty engineering officer, electronics technician, and officer of the deck are all required to follow well-defined procedures before work aloft may commence. These procedures are defined in the *Standard Organization and Regulations of the U.S. Navy,* OPNAVINST 3120.32 series and in the *Navy Safety Precautions for Forces Afloat,* OPNAVINST 5100.19 series. Each ship will provide additional instructions. The commanding officer (CO) accomplishes this in the ship's organization and regulation manual.

In most ships it is required that the division planning work aloft obtain the concurrence of the communications watch officer, combat information watch officer, and duty engineering officer, and the permission of the officer of the deck. Those who violate these instructions subject themselves to disciplinary action. Enforcement is the necessary adjunct to safety consciousness. EMOs must not only develop among the technicians a positive attitude that safety rules are in the common interest, they must enforce the regulations that ensure safety.

Doing a job the safe way in some cases may take a little longer or may be a little less convenient; however, the importance of doing all work in accordance with applicable safety precautions cannot be overemphasized.

SAFETY REQUIREMENTS IN WORK AREAS

Safety requirements concerning the various shop and work areas aboard ship are prescribed by the *Naval Ships' Technical Manaul* (NSTM), the EIMB *General Handbook,* and other authorities.

The following information is a guideline to check the safety of electronic spaces.

Rubber Matting

Rubber matting (requirements are outlined in the NSTM, chapter 634), is to be provided on the deck around electrical and electronic equipment which may be contacted by personnel servicing or tuning the equipment, and on areas in front of workbenches or tables in electrical and electronic shops. Such matting may be cemented to the deck, except on gratings or removable deck plates.

To ensure that the safety factors included in the manufacture of the material are effective, and that the matting is completely safe for use, operation and maintenance personnel must make certain that all foreign substances, which could possibly contaminate or impair the dielectric properties of the matting material, are promptly removed from its surface areas.

For this reason, a scheduled periodic visual inspection procedure and cleaning practice should be established. During visual inspection, personnel should make certain that the dielectric properties of the matting have not been impaired or destroyed by oil impregnation, piercing by metal chips, cracking, or other defects. If it is apparent that the matting is defective for any reason, a replaceable section of matting material should be employed to cover the area affected (see the NSTM, chapter 634).

Additional Safety Requirements

Make sure all switches and circuit breakers are open and tagged prior to working on equipment. Before energizing equipment after the tags are removed, be sure all personnel are notified and are clear. OPNAVINST 3120.32 series outlines tag-out procedures for all equipment. Basically, the procedures are for the protection of personnel and equipment, and for the safety of the ship. Caution, Danger, Out-of-Commission, and Out-of-Calibration tags are hung or affixed to equipment to alert personnel that special circumstances exist for the concerned equipment and that operation or use of the equipment is potentially dangerous to life, equipment or the ship. The equipment's existing condition shall NOT be altered in any way, nor depended upon in the case of Out-of-Calibration tags, without approval of the authorizing officer. Each ship has a tag-out bill that provides tag-out rules, explains the tag-out tag and specifies authority for each tag-out condition. Proper tag-out usage is the last line of defense

against injury and fatalities from improper equipment operation. It is the EMO's responsibility to insure compliance with all provisions of the tag-out bill.

Use one hand only when working on energized circuits—and never work alone.

"Danger high-voltage" signs, safety precautions, artificial respiration instruction, and operating instruction signs are to be posted in all areas containing major units of electronic equipment.

"Danger stack gas" warning signs, "Warning rf radiation hazard," and "Danger high-voltage" signs must be posted at prominent locations in the mast area.

"No smoking" signs are to be posted in spaces where storage batteries are charged and all other spaces where explosive vapors may be present.

Rubber insulating gloves rated at 5,000 V must be readily available to electronics personnel. (See *General* EIMB, Section 3 and *Naval Ships Technical Manual* (NSTM), Chapter 300 for more details.)

Shorting probes are to be made available in all spaces. These are standard stock items rated at a minimum of 25 kilovolts. (See the *General* EIMB, Section 3 for a description of safety shorting probes.)

Lineman's gloves and goggles must be available for handling cathode-ray tubes.

A proper safety harness is to be available for working aloft or over the side (see the EIMB, *General Handbook,* Section 3). Working aloft is discussed in the EIMB and in the *Navy Safety Precautions for Forces Afloat,* OPNAVINST 5100.19 series.

Portable carbon dioxide (CO_2) fire extinguishers must be readily available in all electronics areas.

Spaces are not to be used for unauthorized stowage.

There must be an operational communications system between all electronic spaces.

All portable electronic equipment and tools must be equipped with approved three-prong plugs except for double insulated tools (See NAVOP 161744Z, Nov 79).

There must be adequate emergency lighting.

Radioactive tubes are to be properly identified and stowed. See *General* EIMB, Section 3 for details on stowage.

Provisions must be made for proper disposal of broken or unbroken radioactive tubes in each space where these tubes are being used.

If a situation should arise where an electron tube containing radioactive material is broken, the step or procedure for cleaning the area are covered in the *General* EIMB, Section 3. A radioactive spill kit with all the materials to clean the area quickly and properly would be an asset. The ship should have at least one (1) radioactive spill disposal kit for electronic spaces. More may be required depending on the number and location of electronic spaces in which radioactive tubes are used or stored. The kit should contain the following items:

1. Container—Must be large enough to hold all clean-up materials and pieces of broken radioactive tubes and be airtight. A three pound coffee can with a plastic lid will serve as a suitable container.
2. Marking—The container shall be clearly marked "RADIOACTIVE SPILL DISPOSAL KIT", and contain an unused standard radioactive decal, to be utilized as required.
3. Rubber gloves—Two pairs of surgical latex gloves are recommended and used to prevent contact with contaminated material.
4. Forceps or hemostats—Used for picking-up large pieces.
5. Masking tape—A roll of two inch wide tape for picking up small pieces.
6. Gauze pads or rags—A stack of four inch gauze pads for wiping down the area. Sponges are <u>not</u> to be used.
7. Container of water—A small container of water (approximately 6 oz) for wetting the gauze pads or rags.
8. Chalk—Used for marking the contaminated area.
9. Surgical masks—Disposable surgical masks may be included for protection from inhalation of dust. At present there are no instructions or regulations requiring the spill disposal kit. It is a requirement put out by the FTG and it is one of the graded exercises you, as EMO, will be required to complete during a battle problem. Be prepared for any and all situations.

Any equipments having multiple source voltages should be provided with a switch mounted as close as practical to the equipment in the space, to disconnect that equipment from its source of power and synchro voltages.

HAZARDS OF ELECTRO-MAGNETIC RADIATION TO PERSONNEL (HERP)

The development of radio-frequency (rf) transmitting systems with high-power transmitting tubes and high-gain antennas has increased the possibility of injury to personnel working in the vicinity of these radiating elements.

An electromagnetic radiation hazard may be considered to exist when civil or military electronic equipments generate an electromagnetic field of sufficient intensity to:

1. Cause harmful or injurious effects to humans and wildlife
2. Induce or otherwise couple currents and/or voltages of magnitudes large enough to initiate electro-explosive devices (EEDs) or other sensitive explosive components of weapons systems, ordnance, or other explosive devices
3. Create sparks having sufficient magnitude to ignite flammable mixtures or materials which must be handled in the affected areas

These hazardous situations can arise when a transmitter or antenna installation generates electromagnetic radiation in the vicinity of personnel, ordnance or fueling operations in excess of established safe levels or increases the existing electromagnetic radiation levels to a hazardous level, or when personnel, ordnance or fueling evolutions are located in an area which can be illuminated by electromagnetic radiation at a level that will be hazardous for the planned operations or occupancy.

Hazards of Electromagnetic Radiation to Personnel

Electromagnetic radiation is hazardous to personnel in two ways. It can cause radio frequency burns (rf burns) and it can cause biological, thermal and neurological effects to personnel (RADHAZ). Due to the differences in characteristics and safety precautions required for each of the two types, they will be discussed separately.

Radio Frequency Burn Hazards To Personnel (rf burn)

An rf burn hazard is a hazardous condition that is caused by the existence of radio frequency (rf) voltages on a ship at places where they are not intended to be and are not normally expected.

Metallic objects having the physical and electrical characteristics of an antenna are commonplace aboard ships. Long lengths of metallic lines are particularly efficient interceptors of rf energy. Since most shipboard hf antennas transmit vertically polarized fields, voltages are more likely to be induced in vertical lines than in lines oriented in other directions. Replenishment ships are more likely to encounter the rf burn problem than other types of ships, although the problem is not exclusive with that type. Any type of ship with high-power hf transmitters is susceptible. Potentially hazardous voltages have been found on lifelines, vertical ladders, ASROC launchers, gun mounts, rigging for underway replenishment, boat davits, and on aircraft spotted on carrier and helicopter flight decks.

As a practical matter, whether an induced voltage creates an rf burn hazard depends upon whether personnel will come into contact with the object being energized. Generally, only the voltage between an object and the deck is important. The rf burn occurs when a person comes into contact with a source of rf voltage in a manner that allows rf current to flow through the area of contact. Resistance of the skin to the current flow at the area of contact causes heat. The effect of the heat on a person at the point of contact ranges from noticeable warmth to a painful burn.

The level of rf voltage that creates a hazardous condition is not distinct. For example, the involuntary reaction of personnel to a non-lethal electromagnetic radiation shock can be extremely dangerous when a person is working in close quarters or in elevated locations since such reflex action can result in falls or bodily injury

from striking an object. For our purposes, "hazardous" will be defined as the rf voltage level sufficient to cause pain, visible skin damage, or involuntary reaction. The term "hazard" does not include the lower voltages that cause annoyance, a stinging sensation, or moderate heating of the skin. The Naval Ship Engineering Center has established that an open-circuit rf voltage exceeding 140 volts on an object in an rf radiation field is to be considered hazardous.

The radio frequency burn hazard warning sign shown in figure 3-3 should be posted in a suitable location in view of deck force personnel, at the foot of ladders or other accesses to all towers, masts and superstructure areas which have hazardous levels of radiation. It warns that: "A radio frequency burn hazard may exist to personnel contacting ungrounded wire ropes, rigging and unrep lines near transmitting antennas."

While there is no universally applicable method to completely eliminate rf burn hazards, there are several approaches to eliminating the problem in some cases or, in other cases, reducing it to manageable proportions.

One method of eliminating the rf burn hazard on boom whip and downhaul hooks is to install an insulator link between the rigging and the hook. Such insulators are available through the National Stock System. Unfortunately, numerous equipments involved in the rf burn problem are not amenable to the use of an insulating link.

Another approach being pursued is the use of non-metallic materials for applications where the rf burn hazard is a problem. Objects that can be made of non-conducting material will not be susceptible to induced voltages and will insulate personnel from contacting adjacent voltages on metallic items. At present though, there is no suitable non-metallic substitute for the wire rope used on cranes and replenishment equipment.

The most useful and widespread technique in the reduction of rf burn hazards is the proper bonding and grounding of all metallic objects in the rf radiation field. Typical items include removable stanchions and ladders, standing rigging, boat davits, cargo booms and associated tackle. Specification and examples of shipboard bonding and grounding may be found in military specification *Shipboard Bonding, Grounding, and Other Techniques for Electromagnetic Compatibility and Safety* MIL-STD-1310 series.

In some cases, the rf burn hazard can be eliminated only through the use of restrictive operating procedures that govern the simultaneous use of the transmitting and cargo equipments. These procedures incorporate the use of techniques such as operation of transmitters at reduced power and the prohibition of simultaneous use of certain combinations of antennas, frequencies and cargo handling equipments.

BIOLOGICAL, THERMAL AND NEUROLOGICAL EFFECTS TO PERSONNEL (RADHAZ).—RADHAZ refers to the direct illumination of personnel by high power microwave electromagnetic radiation. The primary sources of shipboard RADHAZ problems are radars. Missile control radars are the most hazardous of all radars as they combine high power transmitters with high-gain narrow-beam antennas. Power densities as high as 300 mW/cm^2 (milliwatts per square centimeter) may be achieved.

Search, missile and fire control radars are located to give maximum unobstructed coverage; however, antenna height is limited because of weight considerations. While radars are not normally hazardous as long as their antennas are rotating and/or scanning, many radars can radiate with the beam stationary and thereby be hazardous. For example, most missile control directors can be positioned throughout 360° azimuth and from $-25°$ to $+90°$ elevation. In these cases, even though the antenna is mounted high, many areas of the main deck and superstructure can be illuminated by the main beam.

By far, the emphasis on the subject of radiation hazards (RADHAZ) has been directed toward the impact of electromagnetic radiation on man because of the biological, thermal and neurological effects that occur in human organs and other biological tissues. Certain organs of the body are considered to be more susceptible than others to the effects of electromagnetic radiation. Presently available information and

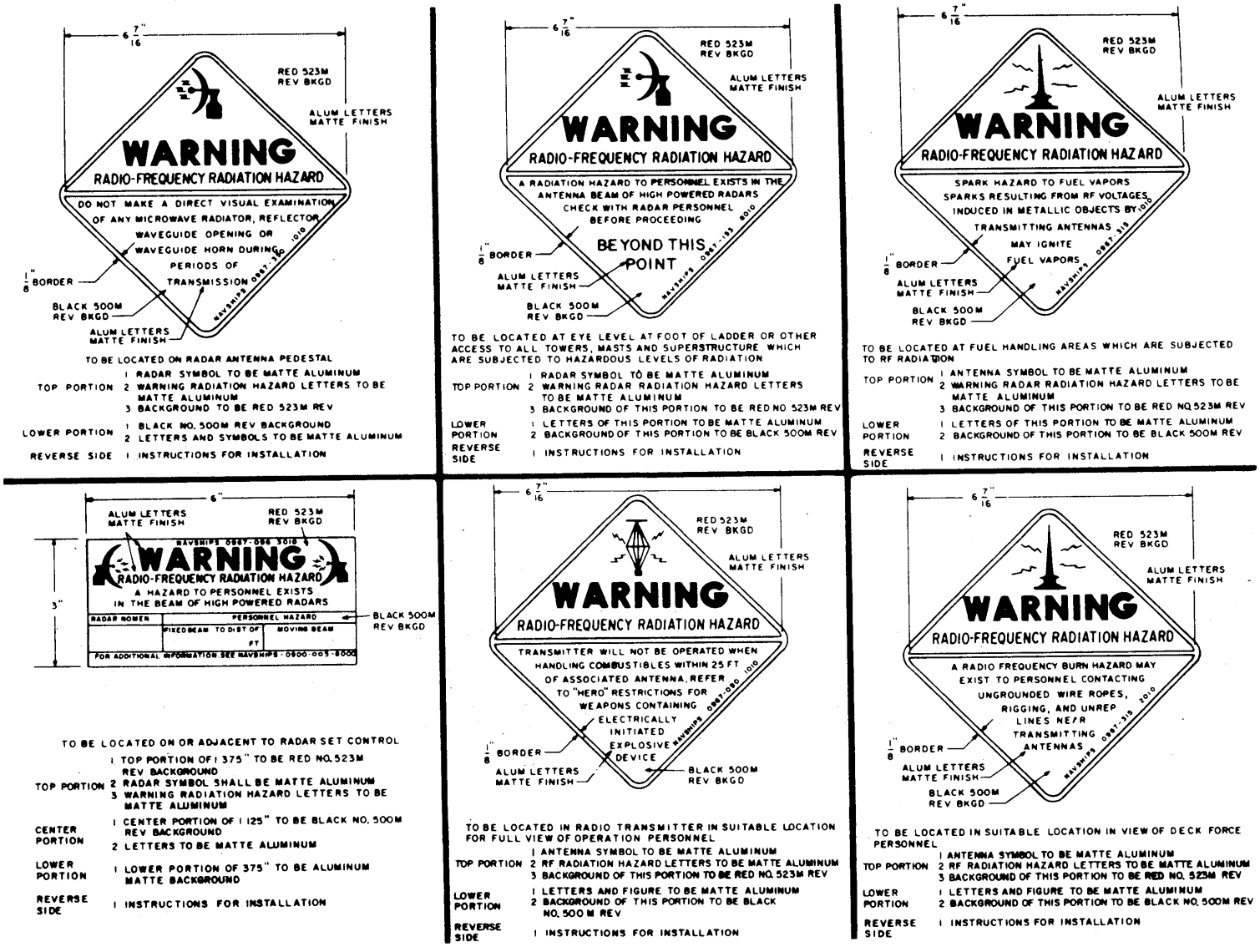


Figure 3-3.—Examples of rf radiation warning signs.

experience indicate that the eyes and testes are the most vulnerable body organs to microwave radiation. The overwhelming danger to date appears to be the hazard from thermal effects which are a function of intensity of radiation and frequency, particularly in the range of 1 to 3 GHz. Thermal effects appear to taper off in severity outside this range.

When the body is irradiated by energy from a point source, the total body surface is usually not exposed. The larger the area exposed and the larger the radiation power density, the higher the body temperature rise and the greater the hazard. Microwave radiation from a radar source will "cook" you internally, just as a microwave oven would cook a chicken.

An injury of great concern is that to the lens of the eye. Exposure of the lens to high-intensity microwaves may cause cataracts. Current medical evidence indicates that a significant temperature elevation of the lens is required for cataract formation. If exposure is limited to 10 mW/cm^2, the lens temperature is not elevated to levels at which cataractogenesis occurs.

In addition to thermal effects, nonionizing radiation is known to produce nonthermal effects. An association of a biological hazard with the nonthermal effects has not been demonstrated.

A peculiar effect experienced by some personnel is the sensation of sound when they are exposed to pulsed microwave fields. This occurs at levels below stated hazard limits and is not, by itself, considered dangerous.

The Bureau of Medicine and Surgery in BUMED Instruction 6470.13 series has established safe limits based on the power density of the radiation beam and the exposure time of the human body in the radiation field. Exposure limits are defined in the following sections.

CONTINUOUS EXPOSURE.—Personnel shall not be exposed to a power density which, when averaged over any 0.1-hour period, exceeds 10 mW/cm^2 in the frequency domain of 10 MHz to 100 GHz. Neither the root mean squared electric field strength (E) nor the root mean squared magnetic field strength (H) may exceed the following values when averaged over any 0.1-hour period:

$$E = \frac{200 \text{ Volts}}{\text{Meter}}$$

$$H = \frac{0.5 \text{ Ampere-turns}}{\text{Meter}}$$

(These are the electric and magnetic field strengths roughly corresponding to electromagnetic waves in free space to which a value of power density of 10 mW/cm^2 may be assigned.)

INTERMITTENT EXPOSURE.—For a condition where exposure is not regular in time or continuous in level over the 0.1-hour period, the equivalent energy fluence level of 1 $mW\text{-}hr/cm^2$ may be used as the limit of exposure for any 0.1-hour period. In situations where measurements of two or more quantities are available, the most restrictive shall be used as the limiting factor.

All areas in which the rf levels exceed the safe limits must be considered hazardous.

Responsibility

The Naval Sea Systems Command is responsible for determining hazardous shipboard areas and ensuring that the possibility of biological injury to personnel from rf radiation is minimized or nonexistent. Theoretical calculations and power density measurements are used to establish outer boundaries from radar antennas. It is not biologically safe for personnel to enter these boundaries. This information, together with additional power density measurements, if necessary, is then used to determine if and where hazardous shipboard areas exist. Cam cutouts (trigger kills) are installed to minimize the number of hazardous areas. These are electrical and/or mechanical devices which inhibit radar transmitter radiation through work areas. All hazardous areas subject to entry by personnel are posted with warning signs, and the ship interior communication system is used to warn personnel if radars are abnormally hazardous.

Electromagnetic Environment

Electromagnetic radiation can be neither seen nor sensed. Therefore, its presence must be measured by use of special sensitive instruments or by theoretical calculations, so that the safety of personnel involved in various activities within the electromagnetic environment is assured. The importance of remaining alert to the danger of overexposure to electromagnetic radiation is emphasized.

Hazards to personnel come from continuous or intermittent exposure to main beam radiation. Table 3-2 is an excerpt from NAVSEA OP 3565/NAVAIR 16-1-529/NAVELEX 0967-LP-624-6010, *Electromagnetic Radiation Hazards,*

Table 3-2.—Personnel Hazards from Continuous or Intermittent Exposure to Main Beam Radiation

TRANSMITTER	MODE	FIXED BEAM HAZARD			MOVING BEAM		
		DISTANCE		MAX. EXP. TIME	PERSONNEL HAZARD	DISTANCE	
		METERS	FEET			METERS	FEET
SHIPBOARD AND SHORE STATION EQUIPMENT (Continued)							
AN/SPS-37A		14	45	0	NO	-	-
AN/SPS-38		15	50	0	NO	-	-
AN/SPS-39,A		120	400	1	NO	-	-
AN/SPS-40,A,B		18	60	1	NO	-	-
AN/SPS-41		NO HAZARD		6	NO	-	-
AN/SPS-42		55	180	1	NO	-	-
AN/SPS-43		21	70	0	NO	-	-
AN/SPS-43A		14	45	0	NO	-	-
AN/SPS-45		14	45	0	NO	-	-
AN/SPS-46		NO HAZARD		6	NO	-	-
AN/SPS-48**		250	840	0	NO	-	-
AN/SPS-49		61	200	1	NO	-	-
AN/SPS-51		NO HAZARD		6	NO	-	-
AN/SPS-52		130	440	0	NO	-	-
AN/SPS-53,A,E		NO HAZARD		6	NO	-	-
AN/SPS-55		8	25	0	NO	-	-
AN/SPS-57		NO HAZARD		6	NO	-	-
AN/SPS-58		NO HAZARD		6	NO	-	-
AN/SPS-58A		2	8	4	NO	-	-
AN/SPS-58C		2	5	4	NO	-	-
AN/SPS-63		NO HAZARD		6	NO	-	-
AN/SPS-65		8	25	4	NO	-	-
AN/SPS-67		11	35	1	NO	-	-
AN/SPW-2A,B		NO HAZARD		6	N/A	-	-
AN/SSC-6		240	800	0	N/A	-	-
AN/TPN-8		14	45		N/A	-	-
[illegible]		[illegible] HAZ[illegible]			[illegible]/A		

which provides guidance in determining hazardous areas in the vicinity of radar transmitters. This table is not representative of all types of radar transmitters. The EMO should review all three parts of the text for complete listings.

While every effort must be made to protect personnel from harmful exposure to rf radiation, it is not considered necessary or desirable, in general, that blanket restrictions on ship antenna radiation be imposed to achieve this end. Such a policy tends to restrict maintenance and checkout procedures which could otherwise be carried out in safety, provided proper precautions are taken to keep personnel clear of hazardous intensity levels. Some of these precautions follow.

PRECAUTIONS.—Visual inspection of feed horns, open ends of waveguides, and any opening emitting rf electromagnetic energy will not be made unless the equipment is definitely secured for the purpose of such an inspection.

Aircraft employing high-power radars must be parked, or the antennas oriented so that the beam is directed away from personnel work areas.

When operating or servicing a shipboard radar, operating and maintenance personnel must observe all rf radiation hazard signs posted in the operating area. This is to ensure that the radar is operating in such a manner that personnel on deck or in the superstructure of the ship, or personnel working on or operating pier or dock cranes are not subjected to hazardous levels of rf radiation. Examples of these signs are shown in figure 3-3.

Train and elevate nonrotating antennas away from inhabited areas, ships, piers, dry dock and pier cranes, and such, while radiating.

Where possibility of accidental exposure might still exist, require technical personnel to have someone stationed topside, within view of the antenna (but well out of the beam), and in communication with the operator, while the antenna is radiating.

Ensure that radiation hazard warning signs are available and used, not only where required to be permanently posted, but also for temporarily restricting access to certain parts of the ship while radiating.

HAZARDS OF ELECTROMAGNETIC RADIATION TO ORDNANCE (HERO)

Modern radio and radar transmitting equipment produces high-intensity radio-frequency (rf) fields. Such fields can cause premature actuation of sensitive electroexplosive devices (EEDs) contained in ordnance systems. The Hazards of Electromagnetic Radiation to Ordnance (HERO) problem was first recognized in 1958 and prime factors causing the problem have been increasing ever since. The use of EEDs in ordnance systems has become essential; while, at the same time, the power output and frequency ranges of radio and radar transmitting equipment are continually being extended.

It is possible for rf energy to enter an ordnance item through a hole or crack in its skin or to be conducted into it by firing leads, wires, screwdrivers, and the like. In general, ordnance systems that have proven to be susceptible to rf energy are most susceptible during assembly, disassembly, loading, unloading, and handling in rf electromagnetic fields.

The most likely effects of premature actuation are propellent ignition or reduction of reliability by dudding. Where out-of-line safety and arming (S&A) devices are used, the actuation of an EED may be undetectable without disassembly. In the absence of such S&A devices, or in the event rf energy bypasses the devices, there exists the probability of warhead detonation. Table 3-3 provides an example of data that may be obtained from the texts referenced in the following paragraphs.

INFORMATION SOURCES ON RESOURCES FOR HAZARDS OF ELECTROMAGNETIC RADIATION TO PERSONNEL (HERP), FUEL AND OTHER FLAMMABLE MATERIAL (HERF), AND ORDNANCE (HERO)

A primary source of directives and other guidance for HERP, HERF, and HERO for the electronics material officer can be found in NAVSEA OP 3565/NAVAIR 16-1-529/ NAVELEX 0967-LP-624-6010, *Electromagnetic*

Table 3-3.—HERO Separation Distances from Transmitting Equipments

EQUIPMENT	HERO UNSAFE ORDNANCE		HERO SUSCEPTIBLE ORDNANCE	
	METERS	FEET	METERS	FEET
AN/SPS-30	1637	5370	1162	3810
AN/SPS-31	1402	4600	488	1600
AN/SPS-32, XN-1	2561	8400	549	1800
AN/SPS-33 Long Range	1555	5100	1098	3600
AN/SPS-35	9	30	9	30
AN/SPS-36	3	10	3	10
AN/SPS-37	2104	6900	457	1500
AN/SPS-37A	3475	11400	777	2550
AN/SPS-39, -39A	960	3150	686	2250
AN/SPS-40	960	3500	351	1150
AN/SPS-41	3	10	3	10
AN/SPS-42	976	3200	686	2250
AN/SPS-43	1884	6180	439	1440
AN/SPS-43A	3476	11400	777	2550
AN/SPS-45	473	1550	220	720
AN/SPS-45, XN-1	494	1620	201	660
AN/SPS-46, -46X	9	30	9	30
AN/SPS-48	1951	6400	1372	4500
AN/SPS-49	1585	5200	671	2200
AN/SPS-51	3	10	3	10
AN/SPS-52	915	3000	655	2150
AN/SPS-53, -53A, -53E	9	30	9	30
AN/SPS-55	29	95	21	70
AN/SPS-57	3	10	3	10
AN/SPS-58	140	460	79	260
AN/SPW-2A, -2B	14	45	11	35
AN/SRC-10	137	450	15	50
AN/SRC-11	137	450	15	50
AN/SRC-12	46	150	6	20
AN/SRC-16	2439	8000	244	800

Radiation Hazards, Volume I and Volume II, Parts One and Two.

Volume I supplies data on the hazards of rf, laser, and ionizing radiation to personnel, and the hazards of rf to fuel. Volume II provides the necessary information on the hazards of rf radiation to ordnance systems/items. Part one of volume II is unclassified and lists all ordnance systems/items covered in both parts of the volume. Part two provides detailed information on the ordnance systems/items that are classified for security reasons.

The contents of both volumes include procedures and precautions necessary to prevent

injury to personnel, premature initiation of ordnance containing electroexplosive devices (EEDs) and accidental spark ignition of fuel vapors. In addition, the safe distances from shipboard and shore transmitters are listed, and the radiation patterns and safe distances from aircraft transmitters are illustrated. Appendicies are supplied to describe the biological effects of exposure to radiation and provide the definitions of terms used in the manual. Lists of the documents referenced in the manual that supply supplementary data and samples of emission control (EMCON) bills show the user how to prepare safety instructions for personnel involved in certain operations.

The manual shall be used by the following types of naval activities:

a. Naval ordnance stations

b. Naval weapons stations

c. Naval magazines

d. Naval ordnance facilities

e. Naval air stations

f. Naval air facilities

g. Marine Corps air stations

h. Marine Corps bases

i. Submarine support facilities

j. Naval stations

k. Naval shipyards

l. Naval ships

The general content of each of the chapters in Electromagnetic Radiation Hazards, Volume I, is shown in the following listing:

Chapter 1—Introduction

Chapter 2—Radio-frequency hazards to personnel

Chapter 3—Radio-frequency burns

Chapter 4—Hazards of microwave ovens

Chapter 5—Laser operation, safety procedures, and safe exposure levels (fig. 3-4)

Chapter 6—Ionizing radiation sources, hazard levels, and safety precautions

Chapter 7—Procedures to reduce possibility of fuels being ignited by rf radiation induced arcing

Volume II, part one, lists Navy and Marine Corps ordnance with their HERO classifications and detailed instructions for their proper handling in rf fields. If the ordnance has a security classification, the detailed instructions are supplied in volume II, part two.

Authority and Responsibility of Supervisors

Supervisors are to be thoroughly familiar with the provisions outlined in Electromagnetic Radiation Hazards. Supervisors have no authority to waive or alter NAVSEASYSCOM and station safety regulations nor are they to permit the violation of such safety regulations by others. They are to act positively to eliminate any potential accident hazards existing in operations under their jurisdiction. Aboard ship supervisory personnel must perform the functions of a shore station safety director. All supervisors are to comply with the following regulation.

1. Supervisors must explain to all personnel under their immediate supervision the standard safety regulations, industrial hygiene safeguards, and precautions that must be followed. Supervisors must enforce these safety regulations. Supervisors also must explain safe distances as they apply to rf energy, microwave ovens, and lasers.

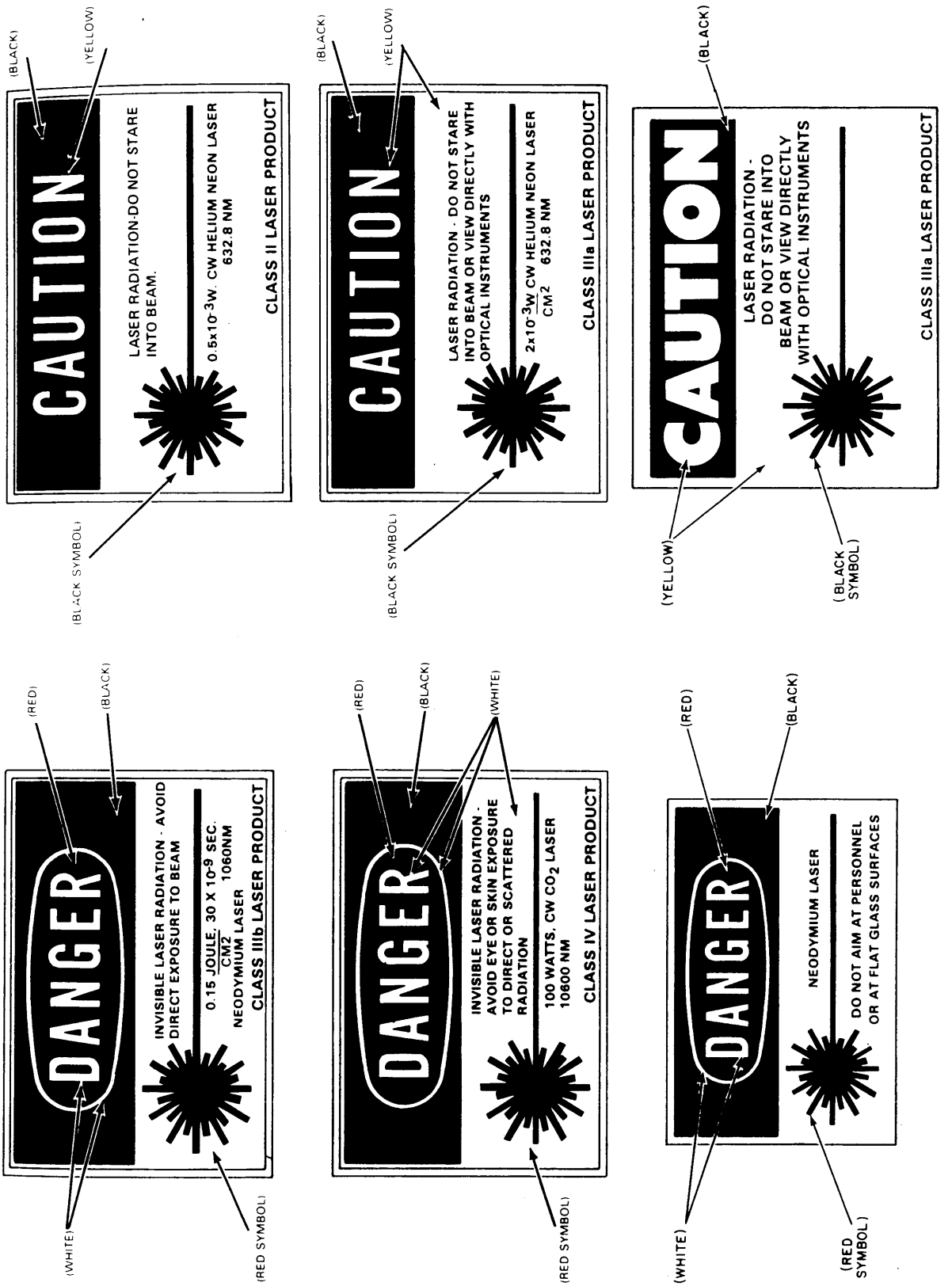


Figure 3-4.—Laser warning signs.

2. Supervisors are to instruct and train personnel under their immediate supervision in the work that they are to perform, whether instruction is given directly or through experienced operators, until the supervisors are satisfied that all personnel are capable of performing the work safely. This instruction also is to encompass complete information concerning transmitter location; identification; adherence to all rf and laser warning signs (fig. 3-4) and placards; and observance of all safety circles and other safety zones.

3. Supervisors are to ensure that personnel are qualified and certified to perform the job assigned and that such certification is current. They are to report promptly to their immediate superior, all personnel who, in their opinion, are not qualified for their assigned work.

4. Supervisors must investigate or assist in the investigation of all accidents involving operations, equipment, or personnel under their supervision, and report or assist in the preparation of the report on the investigation's results to higher authority for appropriate action.

5. Supervisors are to identify all persons in their charge who enter or approach a RADHAZ unsafe area and determine their authority to enter and/or remain in the area. Supervisors are to exercise their authority to eject any person whose presence and/or actions, in their opinion, are detrimental to safety.

6. Supervisors are to forbid any major repairs or modification to any transmitting equipment or ordnance, except in accordance with the specific instructions of the commanding officer. They are to enforce the safety requirements in their area.

7. Supervisors must ascertain that all conditions in any area under their jurisdiction comply with orders relating to operation shutdown. When the operation is not relieved by an incoming shift, supervisors must make certain that all transmitters are shut off. When an incoming shift relieves the operation or if they are relieved for any reason, supervisors are to make a complete report to the relief regarding any situation that requires immediate attention or which should be kept under observation.

8. Supervisors must enforce observance of the safety regulations concerning the protective clothing and equipment of personnel.

9. Supervisors are to report in writing to their commanding officer any requests, suggestions, and comments they may have regarding safety standards. Radio-frequency health and HERO information sources are contained in the following list:

Electromagnetic Radiation Hazards, Volume I (Hazards to Personnel Fuel & Other Flammable Material), NAVSEA OP 3565/NAVAIR 16-1-529/NAVELEX 0967-LP-624-6010

Electromagnetic Radiation Hazards (Hazards to Ordnance), Volume II, Part One and Part Two, NAVSEA OP 3565/NAVAIR 16-1-529/NAVELEX 0967-LP-624-6010

Identification of DOD C&E Equipment Capable of Producing Biological Radiation Hazards (DC 750358S)

U.S. Radar Equipment, MIL-HDBK-162B

Instruction Manual for Microwave Radiation Protection Clothing, NAVSEA 0967-LP-316-3010

Electromagnetic Radiation Hazards, MIL-HDBK-238 (NAVY)

SECURITY

Security of the United States in general, and of naval operations in particular, depends in part upon success attained in safeguarding classified information. EMOs must be security conscious to the point that they automatically exercise proper discretion in performing their duties and in overseeing those of their assigned personnel and do not think of security of information 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.

During the daily work routine, the EMOs handle information of vital importance to the military and to the nation. Some of the vast amount of intelligence in messages handled by

naval communications passes at some point through the hands of the EMOs; data which, if available to an enemy, might disclose the strength and intent of U.S. forces, and reveal a wealth of technical information relating to procedures and operations of the United States Navy.

Electronics personnel use many official documents and publications that relate to such matters as frequencies, call signs, specifications, and procedures. These contents must be protected, because the more an enemy knows about these data, the better the chances are of deriving intelligence from them.

Rules and regulations on the subject of security do not guarantee results, nor do they cover every conceivable situation. The law of diminishing returns limits control measures that can be employed profitably. In administering security, a balanced and commonsense outlook must be maintained. All concerned must learn to exercise proper discretion in carrying out assigned duties so that observing proper security precautions becomes an automatic and integral part of the daily routine.

The Navy is a potential source of valuable information, and unceasing, systematic attempts to exploit that source are to be expected. The methods that may be used are many and varied. Planting agents within the naval establishment, photographing or stealing classified documents, tapping telephones and telegraph lines, employing electronic sensing devices which can be used from a distance, obtaining codes and ciphers, and analyzing naval personnel in their off-duty time are some of the procedures which might be used. Although information obtained through these means often appears innocuous, it proves to be of real value when subjected to expert, purposeful analysis and when combined with other fragments of information from various sources.

EMOs hear a great deal about the security of classified material because they have responsibility for overseeing access to classified information every day. For this reason, all activities brief newly arrived personnel on security and require them to sign a statement attesting to the fact that they have received the briefing and understand the contents. Further, as a part of each command's security program, EMOs are required to read and indicate their 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 is only as effective as it is made to be. Security is a basic part of the EMO's assignment. This personal responsibility of an EMO to protect information cannot be transferred to any one else. Security is more than a matter of being careful; it requires both study and practice. Thorough understanding of this chapter will not provide full knowledge of all the finer points concerning security, but it will provide a good fundamental background upon which security is built. The basic reference for security is the OPNAVINST 5510.1 series. Thorough familiarity with this instruction is absolutely essential. Material presented in the SEMO course is, in the main, derived from the OPNAVINST 5510.1 series and is subject to change. As a result, EMOs should consult the actual security instructions and publications for security decisions and guidance.

PURPOSE OF SECURITY PROGRAM

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

Information may be compromised through careless talk, improper handling of classified material, or 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 10054 series.

SECURITY PRINCIPLES

The Department of Defense security formula is based on the premise of circulation control; i.e., the control of dissemination of classified information. According to this policy, knowledge or possession of classified security information is permitted only to persons whose official duties require access in the interest of promoting

national security and only if they are determined to be trustworthy.

DEFINITIONS OF SECURITY TERMS

OPNAVINST 5510.1 series lists the definitions for currently used security terminology. It is imperative that all personnel speak the same security language. See chapter 1 of OPNAVINST 5510.1 series for these definitions.

SECURITY AREAS

Spaces containing classified matter are known as security areas. These security (or sensitive) areas have varying degrees of security interest, depending upon thier purpose and the nature of the work and information or materials concerned. Consequently, the restrictions, controls, and protective measures required vary according to the degree of security importance. To meet different levels of security sensitivity, there are three types of security areas—exclusion, limited, and controlled. All areas are clearly marked by signs reading "RESTRICTED AREA—KEEP OUT. AUTHORIZED PERSONNEL ONLY."

EXCLUSION AREA

A space requiring the strictest control of access is designated an exclusion area and is so marked. This area contains classified matter of such a nature that, for all practical purposes, admittance to the area permits access to the material.

An exclusion area is fully enclosed by a perimeter barrier of solid construction. Exits and entrances are guarded, or secured and alarm protected, and only those persons whose duties require access and who possess appropriate security clearances are authorized to enter.

LIMITED AREA

A limited area is one in which the uncontrolled movement of personnel permits access to the classified information therein. Within the area, access may be prevented by escort and other internal controls.

The area is enclosed by a clearly defined perimeter barrier. Entrances and exits are either guarded, controlled by attendants to check personal identification, or under alarm protection.

Operating and maintenance personnel who require freedom of movement within a limited area must have a proper security clearance. The commanding officer may, however, authorize entrance of persons who do not have clearances. In such instances, escorts or attendants and other security precautions must be used to prevent access to classified information located within the area. The combat information center is classified a limited area.

CONTROLLED AREA

A controlled area does not contain classified information. It serves as a buffer zone to provide greater administrative control and protection for the limited or exclusion areas. Thus, passageways or spaces surrounding or adjacent to limited or exclusion areas may be designated and marked controlled areas.

Controlled areas require personnel identification and control systems adequate to limit admittance to those having bona fide need for access to the area.

CATEGORIES OF CLASSIFIED INFORMATION

TOP SECRET

The Top Secret classification refers to national security information or material requiring the highest degree of protection. It is applied only to information or material of which the defense aspect is paramount, and of which the unauthorized disclosure could reasonably be expected to cause EXCEPTIONALLY GRAVE DAMAGE to the Nation, such as—

1. A war, an armed attack against the United States or her allies, or disruption of foreign relations vitally affecting the national security of the United States.
2. The unauthorized disclosure of military or defense plans, intelligence operations, or scientific or technological developments vital to the national security.

SECRET

The Secret classification is limited to national security information or material which requires a substantial degree of protection, and of which the unauthorized disclosure could reasonably be expected to cause SERIOUS DAMAGE to the Nation, such as—

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

CONFIDENTIAL

The use of the Confidential classification is limited to national security information or material which requires protection, and of which the unauthorized disclosure could reasonably be expected to cause IDENTIFIABLE DAMAGE to the national security, such as—

1. Operational and battle reports that contain information of value to the enemy.
2. Intelligence reports.
3. Military radio-frequency and call sign allocations that are especially important, or are changed frequently for security reasons.
4. Devices and material relating to communication security.
5. Information that reveals the strength of the land, air, or naval forces in the United States and overseas areas; identity or composition of the units; or detailed information relating to their equipment.
6. Documents and manuals containing technical information used for training, maintenance, and inspection of classified munitions of war.
7. Operational and tactical doctrine.
8. Research, development, production, and procurement of munitions of war.
9. Mobilization plans.
10. Personnel security investigations and other investigations, such as courts of inquiry, which require protection against unauthorized disclosure.
11. Matters and documents of a personal or disciplinary nature, which, if disclosed, could be prejudicial to the discipline and morale of the armed forces.
12. Documents used in connection with procurement, selection, or promotion of military personnel, the disclosure of which could violate the integrity of the competitive system.

NOTE: Official information of the type described in paragraphs 10, 11, and 12 is classified Confidential only if its unauthorized disclosure could reasonably be expected to cause damage to the security interests of the nation. If such information does not relate strictly to defense, it must be safeguarded by means other than the Confidential classification as indicated in the following text.

SPECIAL MARKINGS

In addition to the security labels mentioned already, other markings also appear on classified material. Among these markings are such designations as "Restricted Data" and "For Official Use Only."

Restricted Data

All data concerned with the (1) design, manufacture, or utilization of atomic weapons; (2) production of special nuclear material; or (3) use of special nuclear material in production of energy bear conspicuous "Restricted Data" markings. Restricted data, when declassified under the Atomic Energy Act of 1954, must be marked "Formerly Restricted Data, Handle as Restricted Data in Foreign Dissemination, Section 144b, Atomic Energy Act, 1954."

For Official Use Only

The term "For Official Use Only" (FOUO) is assigned to official information that requires some protection for the good of the public interest but is not safeguarded by classifications used in the interest of national security.

PREPARATION AND MARKING

Each document or piece of material is classified according to the importance of the information it contains or reveals. It is important to identify individually items of information which require protection and then to consider whether compromise of the document or material as a whole would create a greater degree of damage than compromise of the items individually. The classification of the document or material must be the classification that provides protection for the highest classified item of information or for the document or material as a whole, whichever is higher.

The markings required for classified material serve to record the proper classification, to inform recipients of the assigned classification, to indicate the level of protection required, to indicate the information that must be withheld from unauthorized persons, to provide a basis for derivative classification, and to facilitate downgrading and declassification actions.

Upon assignment of a classification category to information, it is immediately marked clearly and conspicuously on all documents.

On documents, the classification marking of TOP SECRET, SECRET, or CONFIDENTIAL is stamped, printed, or written in capital letters that are larger than those in the text or the document. On other types of material, the classification marking is stamped, printed, written, painted, or affixed by means of a tag, sticker, decal, or similar device in a conspicuous manner. If marking on the material is not physically possible, written notice of the assigned classification is provided to recipients of the material.

CHANGE IN CLASSIFICATION

When classified information is determined to require a different level of protection than that presently assigned, or no longer to require protection, it is regraded or declassified.

A mandatory continuing program based on a time schedule has been established for automatically downgrading and declassifying documents originated within the Department of Defense.

The automatic downgrading and declassification system was instituted to ensure that all classified matter is available to the general public when secrecy is no longer necessary. It also relieves the originators of future concern for the classified aspects of documents or materials they have produced.

Depending on the contents on the material, classified information is placed into one of four groups. The assigned grouping indicates whether the material may be declassified automatically in the future. It also indicates when it may be declassified.

TRANSMISSION

Transmission is the actual transfer of custody and responsibility for a document or other material (often classified) from one command to another command or other authorized addressee.

Although transmission may be accomplished by messenger, mail, wire circuits, secure radio, or other means, the purpose in every case is to keep the information out of the hands of those not authorized to have it.

The most appropriate means of transmission should be selected within the requirements of precedence and security.

MESSENGER

Classified matter is transmitted by messenger when security—not speed—is the paramount objective. The principal messenger agency for the Department of Defense is the Armed Forces Courier Service (ARFCOS). This agency is responsible for the safe transmittal of highly classified matter to military addressees and certain civilian agencies throughout the world. The ARFCOS transfer stations are located in designated areas. Every item of classified material sent via ARFCOS is in the physical custody and control of a military courier from the time of its entry into the system until the addressee or an authorized representative accepts receipt of it. Classified material that may go by registered United States mail is not transmitted by ARFCOS.

MAIL

In addition to transmitting unclassified material, the United States postal system is used to transmit classified material, except Top Secret matter and cryptographic aids and devices. Secret matter must be sent by registered mail instead of by ordinary mail, and must not enter a foreign postal system. Confidential material can be mailed through the United States Postal Service certified or first class mail within United States boundaries. United States Postal Service registered mail is to be used for (1) Confidential material of NATO, SEATO, and CENTO; (2) APO or FPO addressees; and (3) other addressees when the originator is uncertain that their location is within United States boundaries. The single exception to this is that material addressed to Canadian Government activities is permitted to pass through the Canadian postal service. The great bulk of the Navy's administrative traffic is sent by mail, thus reserving radio circuits for operational traffic insofar as possible.

Mailable Secret and Confidential material is double wrapped; the classified material is sealed inside an opaque container which is then sealed within a second opaque container. The inner container shows the address of the receiving activity, the classification of the enclosed material (including special markings), and any applicable special instructions. It is carefully sealed to minimize the possibility of access without leaving evidence of tampering. The outer container shows the address of the receiving activity and the correct return address of the sender. The outer container DOES NOT bear a classification marking. Top Secret mail is prepared for transmission in a similar manner, but is NOT transmitted by mail, since it must be transmitted under a continuous chain of receipts.

TRANSMISSION SECURITY

Transmission security includes all measures designed to protect transmission from interception, traffic analysis, and imitative deception. Every means of transmission is subject to interception. In radio transmission, it must be assumed that all transmissions are intercepted.

Within requirements of precedence and security, the most appropriate means of transmission should be selected. Following are the usually available means of transmission, in order of security: (1) messenger, (2) registered mail, (3) approved wire circuit, (4) ordinary mail, (5) nonapproved wire circuit, (6) visual, (7) sound system, and (8) radio.

SPEED VERSUS SECURITY

Three fundamental rquirements of a military communication system are reliability, security, and speed. Reliability is always paramount. Security and speed are next in importance and, depending on the stage of an operation, are interchangeable. During the planning phase, for instance, security is obviously more important than speed; during the execution phase, speed may possibly surpass security in importance. This statement is not meant to imply that either requirement can ever be ignored completely. Modern high-grade cryptosystems permit security with speed. In tactical operations, however, when speed is so important that time cannot be spared for encryption, and transmitted information cannot be acted upon by an enemy in time to influence current operations, messages of any classification except Top Secret may be transmitted in the clear over any wire or radio circuit. Each message must be approved and released separately. Any linkage to a previously encrypted message should be avoided. Such transmissions include the word CLEAR at the beginning of the test to indicate the message contains classified material. Upon receipt, the message is marked "Received in the clear" and is handled as Confidential. If further information must be transmitted, an entirely new message is drafted.

RADIO TRANSMISSION SECURITY

When a message is transmitted by radio, it sometimes is possible to know a few receivers, but all of them never become known. It must be assumed that an enemy receives every transmission. Properly prepared messages using modern cryptosystems may prevent an enemy from understanding a message, but a lot can still be learned. As time for a planned operation

approaches, for instance, the number of messages transmitted increases markedly. Although unsure of exactly what will happen, an enemy knows that something will occur soon, and enemy forces are alerted accordingly. Strict radio silence is the main defense against radio intelligence.

The amount of radio traffic is not the only indicator used by an enemy. Statistical studies of message headings, receipts, acknowledgments, relays, routing instructions, and services are also run by an enemy. From such studies, communication experts can learn much about an opponent's operations, past and future. By means of direction finders they determine where messages originate, which is a valuable aid in their studies.

Although traffic analysis by the enemy cannot be prevented, it can be made more difficult and less reliable. Such measures as the following can be taken:

1. Make maximum use of communication means other than radio.
2. Maintain strict circuit discipline.
3. Use the broadcast method where possible.
4. Rotate call signs and address groups.
5. Reduce the use of service messages.
6. Use codress messages.
7. Encrypt all classified messages.
8. Reduce test transmission to a minimum.
9. Avoid external routing instructions.

RADIOTELEPHONE SECURITY

Radiotelephone nets are operated so frequently that many operators tend to be careless. There are too many instances of interception of vhf/uhf transmissions at distances of many thousands of miles for this carelessness to continue.

Certain rules apply, and all persons having occasion to use a radiotelephone should be thoroughly familiar with them.

1. Use each circuit for its intended purpose only. Keep the number of transmissions to a minimum.

2. Think out the contents and wording before starting a transmission in order to reveal no information of military value, even by implication.

3. Write the message before transmission, and be practicable.

4. Keep all transmissions brief, concise, and clear.

5. Transmit no classified information in plain language, including plain language references to classified titles, units, places, chart references, or persons that may reveal the nature of the headquarters, task force, or other unit concerned.

6. Avoid linkage between radiotelephone call signs and any other call signs.

7. Follow prescribed radiotelephone procedure at all times.

DESTRUCTION OF CLASSIFIED DOCUMENTS

When it becomes necessary to destroy classified documents, the recommended methods are by burning, shredding, pulping, or pulverizing.

Destruction is accomplished in the presence of one or two witnesses, according to the classification of the material. A witnessing official may be any military or civilian employee having a security clearance at least high as the category of material being destroyed. All persons witnessing must have a security clearance at least as high as the category of material being destroyed, and be thoroughly familiar with the regulations and procedures for safequarding classified information.

When appropriate, certificates of destruction are prepared and signed by witnessing officials. These officials are to observe the complete destruction of the classified documents. The residue of such documents is to be checked to determine if destruction was complete and that reconstruction is impossible. When burning classified material, efforts must be made to ensure that portions of burning material are not carried away by winds or drafts.

A Certificate of Destruction (OPNAV Form 5511-12, Rev. ( )) must be prepared for

nonregistered Top Secret and Secret documents. These certificates are retained for a period of 2 years by the command destroying the material and include a complete identification of the material destroyed and the date of destruction. It also includes the signature of the person authorizing the destruction and the witnessing officials.

In the case of Secret documents only, use of routing sheets, mail logs, and other similar administrative records is authorized in lieu of a Certificate of Destruction, provided all necessary information (identification of material, date of destruction, and signatures of person authorizing destruction and witnessing officials) is included. Confidential documents or documents with a lower classification do not require a Certificate of Destruction.

ROUTINE DESTRUCTION

Destruction of superseded and obsolete classified materials that have served their purpose is termed routine destruction.

Destruction may be accomplished by burning, pulping, pulverizing, or shredding. Burning is the method used most commonly aboard ship.

Every member of the burn detail should know exactly what is to be burned and should doublecheck each item before it is burned. Routine destruction of classified messages and trash generally is handled on a daily basis owing to the rapid accumulation of these materials and the limited space available for storage. To facilitate the complete destruction of classified material, individual pages should be placed loosely into a burn bag prior to burning. For example, bound documents should be torn apart, and the pages crumpled and fed to the fire a few pages at a time. All material must be watched until it is completely consumed. The ashes must be broken up and sifted through to ensure complete destruction. Following complete destruction of the classified matter, the burn log entry is made and the senior person present is required to inspect the ashes and sign as a witness to the destruction. Upon this individual's approval, the ashes are disposed of in accordance with command policy.

EMERGENCY DESTRUCTION

Emergency destruction of classified material is authorized any time it is necessary to prevent its capture by an enemy.

Destruction plans call for the highest degree of individual initiative in preparing for and in actually commencing the required destruction. It is extremely important for all personnel to understand that in emergencies subjecting classified material to compromise through capture, they must start necessary destruction under the plan without waiting for specific orders.

The order in which classified material is to be destroyed under emergency conditions should be determined in advance and the material so marked and stored. The effective edition of the OPNAV Instruction 5510.1 series offers directions about the priority of destruction.

COMSEC material has the highest priority for emergency destruction. Insofar as humanly possible, it must not be permitted to fall into enemy hands. Other classified matter is destroyed in order of classification—highest classification first.

Destruction by fire is the traditional method for all combustible materials. Oil or chemicals may be used to facilitate burning. Classified equipment must be smashed beyond recognition and unclassified equipment should be demolished beyond repair.

A sufficient number of destruction tools—including sledge hammers, screwdrivers, axes, and wire cutters—are always kept in electronics control and equipment spaces for use in emergency destruction. Written instructions regarding emergency destruction for Electronics Divisions must be included in the electronics doctrine and must detail procedures for destruction, location and priority of destruction for software and hardware (using nameplate data), assignment of personnel and alternates by billet numbers, and specific location of destruction devices.

SECURITY VIOLATIONS AND COMPROMISES

When classified information has been lost, compromised, or subjected to compromise,

action is initiated to regain custody of the information and afford it proper protection.

INVESTIGATIVE ACTIONS REQUIRED

Any individual discovering a loss, compromise, or subjection to compromise of classified information reports the facts immediately to the most readily available command.

The command which receives the individual's report takes immediate action to gain custody of the information concerned and affords it adequate protection. An initial inquiry is conducted to identify accurately the information concerned; to determine the circumstances involved in the discovery of the loss, compromise, or subjection to compromise; and tentatively to establish whether the possibility of compromise is remote or substantial. For U.S. Navy and Marine Corps originated classified information, a report of the results of the initial inquiry is sent by rapid means to the command having custodial responsibility for the information concerned. (When the command making the initial inquiry is also the command having custodial responsibility, this report is made to the originator.) Information copies are forwarded to the originator and the Chief of Naval Operations (ACNO (Intelligence)). If the loss or possible compromise is of pages or parts of a classified document (with the exception of registered cryptographic publications), and if the command determines upon initial inquiry that compromise could not have resulted or that possibility of compromise is remote, an information copy of the report need not be furnished to the Chief of Naval Operations.

Upon receipt of the initial inquiry, if further action is required, the command having custodial responsibility makes or arranges for a thorough inquiry into the matter. When circumstances indicate, the investigative services of the nearest Naval Investigative Service Officer should be requested.

After reviewing the record of investigation, the command having custodial responsibility institutes procedures to prevent a recurrence of loss or compromise and takes or recommends disciplinary action, as appropriate, in the case of personnel found responsible.

Upon receipt of the report of initial inquiry advising of the loss, compromise, or subjection to compromise, which may or may not require further action, the originator of the classified information reevaluates all programs, plans, and operations which could in any way be affected by the loss, compromise, or subjection to compromise, in order to determine and implement necessary modification in such programs, plans and operations. The originator promptly notifies all holders of copies of the material, as well as those activities whose programs, plans, or operations could in any way be affected by the loss, compromise, or subjection to compromise, in order that they may undertake reevaluation of the programs, plans, and operations, and implement necessary modifications thereto.

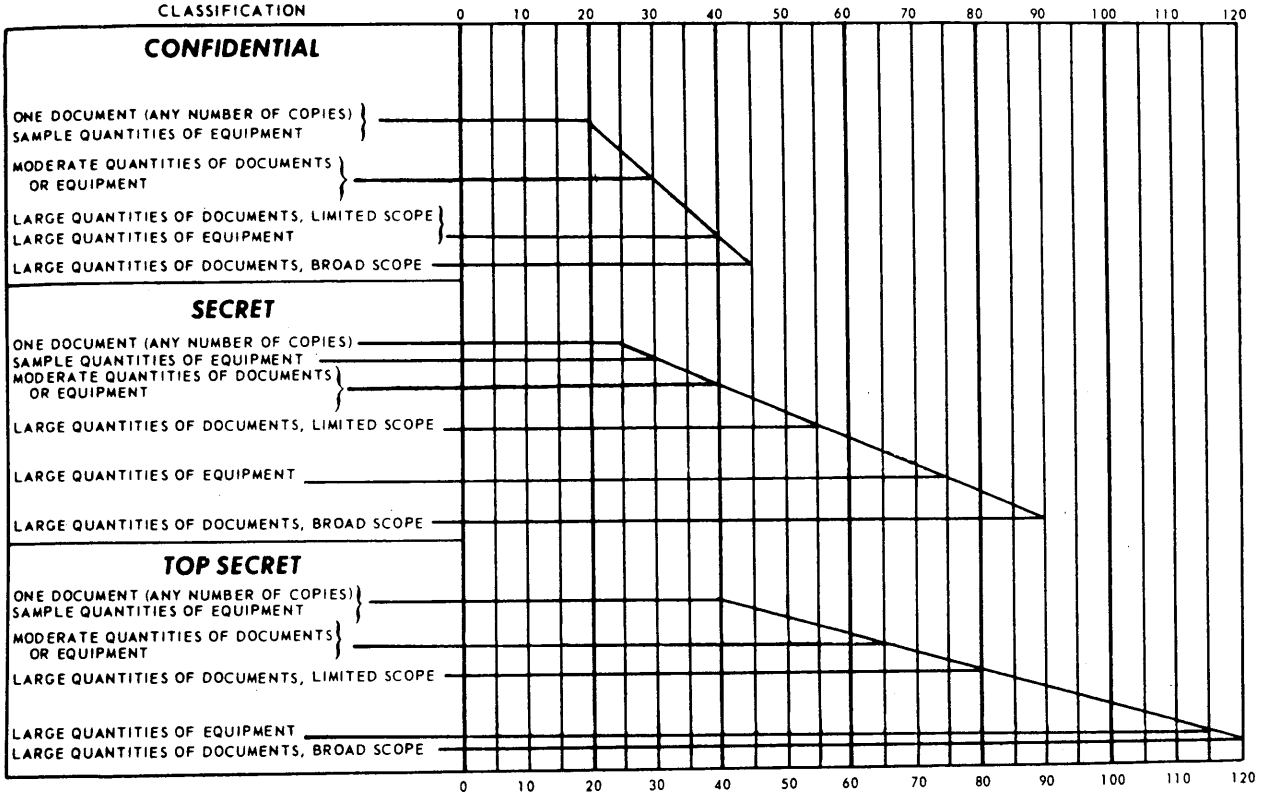
STOWAGE OF CLASSIFIED MATERIAL

All classified matter not in actual use must be stowed in a manner that will guarantee its protection. The degree of protection necessary depends on the classification, quantity, and scope of the material.

A numerical evaluation system has been developed for determining the relationship between the security interest and the level of protection required. The more secure the stowage facilities, the higher the numerical values assigned. Table 3-4 shows the numerical values required for quantity and type of documents of each classification. Table 3-5 is a guide for evaluating stowage facilities. Both of the tables must be used together.

Assume that a ship stows plain language translations of encrypted messages in a metal container with an attached keylock in the cryptocenter. Visitors are not allowed in any of the communication spaces. Only cryptographers may enter the cryptocenter itself or remove anything from its safe. The cryptographer on watch acts as a guard in attendance at the

Table 3-4.—Security of Material in Storage Evaluation Graph



container. From table 3-5 numerical value may be assigned to these facilities as follows:

	Value
Sheltered aboard a commissioned ship	25
Stowed in metal container with attached high security key padlock	5
Military guard in attendance at container	60
Total	90

From the graph in table 3-4 it can be seen that stowage facilities with a numerical value of 90 are secure enough for everything but large quantities of Top Secret equipment and large quantities of Top Secret documents covering a broad scope.

Keys or combinations to safes and lockers containing classified material are made available only to persons whose duties require access to them. At least every 12 months keys or combinations must be changed. There also must be changes whenever any person having knowledge of them is transferred from the organization, and at any time the keys or combinations are suspected of being compromised. A key padlock should also be changed whenever a key is lost.

Any time discovery is made of an unlocked and unattended safe or cabinet that contains classified material, the condition is reported immediately to the senior duty officer. The container or contents are not to be touched; they are to be guarded until the duty officer arrives. The duty officer then assumes responsibility for such further actions as locking the safe, recalling the responsible persons, and reporting the security violation to the commanding officer. The custodian must hold an immediate inventory of the

Table 3-5.—Table of Numerical Equivalents

Element of Security	Value
1. Stowage Areas:	
a. Security Fences:	
(1) Classified area surrounded by a security fence with all gates secured or controlled	5
b. Protective Lighting:	
(1) Security areas lighted by protective lighting	5
c. Building or Ship:*	
(1) Conventional frame or good quality temporary structure	5
(a) Controlled areas within	15
(b) Limited areas within	25
(c) Exclusion areas within	35
(2) Masonry or steel structure with substantial partitions, floors and ceilings (including magazines)	10
(a) Controlled areas within	20
(b) Limited areas within	30
(c) Exclusion areas within	40
(3) Aboard a Commissioned Ship	25
(a) Controlled area	35
(b) Limited area	40
(c) Exclusion area	50
(4) "In Service" or MSC chartered vessel	10
(a) Controlled areas within	20
(b) Limited areas within	30
(c) Exclusion areas within	40
2. Stowage Containers:**	
a. Metal, keylock (built-in)	0
b. Metal, key padlock (attached)	0
c. Metal, high security key padlock (attached)	5
d. Metal, combination padlock (attached)	5
e. Metal, high security combination padlock (attached)	10
f. Metal, combination lock (built-in)	15
g. Strongroom or weapons magazine	15
h. Class C Vault	50
i. Class B Vault	60
j. Class A Vault	70
k. Class 2, approved GSA security container	60
l. Class 3, approved GSA security container	50
m. Class 4, approved GSA security container	60
n. Class 5, approved GSA security container	70
o. Class 6, approved GSA security container	55
p. Class 5 map and plan, approved GSA security container	70
2. Stowage Containers—Continued	
q. Class 6 map and plan, approved GSA security container	55
3. Guarding:	
a. Supporting Guard Force:	
(1) Civilian Supporting Guard Force	10
(2) Military Supporting Guard Force	15
b. Guards:	
(1) Civilian Guards:	
(a) Civilian guard in general area	10
(b) Civilian guard check of container each hour	15
(c) Civilian guard check of container each ½ hour	20
(d) Civilian guard in attendance at container	30
(2) Military Guards:	
(a) Military guard in general area	15
(b) Military guard check of container each hour	20
(c) Military guard check of container each ½ hour	25
(d) Military guard in attendance at container	60
c. Sentry dog accompanying military or civilian guard	10
4. Protective Alarm Systems:	
a. Area Alarm System:	
(1) Make or break (electro-mechanical) alarm to detect entry into immediate area	5
(2) Other alarm system to detect entry into immediate area	10
(3) Alarm system to detect entry or attempted entry into immediate area	15
(4) Alarm system to detect entry or attempted entry and approach to immediate area	25
b. Container Alarm Systems:	
(1) Make or break (electro-mechanical) alarm to detect opening of container	10
(2) Other alarm system to detect opening of container	15
(3) Alarm system to detect opening or tampering with container	20
(4) Alarm system to detect opening or tampering with and approach to container	25

* Buildings must be under U.S. Government control or if not under U.S. Government control the space occupied within the building must be at least a controlled area.

** Evaluate as indicated provided other elements in the security program are available to minimize the possibility of unauthorized access to the container.

contents of the safe and report any loss to the commanding officer.

COMMAND SECURITY PROGRAMS

Security is a means—not an end. Regulations that govern the security of classified material are comparable to electronic safety regulations. They do not guarantee protection, and they do not attempt to meet every conceivable situation. If strictly adhered to, however, they will provide a satisfactory degree of security.

To ensure that the required security measures are implemented, each command formulates written security procedures to reflect the command's particular requirements. These security procedures specify what is to be done, how it is to be done, who is to do it, and who is to supervise it.

In order that classified information may be controlled with maximum efficiency, the commanding officer or officer in charge of each command designates an officer to act as the CLASSIFIED MATERIAL CONTROL OFFICER. In commands that initiate, receive, or process Top Secret documents, a TOP SECRET CONTROL OFFICER is appointed. When an activity possesses crypto material, the commanding officer names a CRYPTOSECURITY OFFICER. In addition, certain commands may designate a SPECIAL SECURITY OFFICER:

The Classified Material Control Officer:

1. Serves as the commanding officer's adviser and direct representative in cases pertaining to security of classified material.

2. Assures that all persons who are to handle classified information are properly cleared and instructed. The clearance status should be recorded and be accessible for verification.

3. Formulates and coordinates security control measures within the command.

4. Maintains a program of declassification and downgrading of information.

5. Prepares classification guides to aid in the proper classification of material originated within the command. Preparation of such guides usually is limited to shore activities.

6. Exercises security control over visits to and from the command.

7. Reviews proposed press releases, and indicates classified information that must be deleted therefrom.

8. Performs the duties of Top Secret (TOPSEC) Control Officer if another officer is not so designated.

The Top Secret Control Officer, subordinate to the classified material control officer, is responsible within the command for the receipt, custody, accountability, and distribution of Top Secret information and for its transmission outside the command. The TOPSEC control officer is governed by certain basic rules, and must, for instance:

1. Avoid unnecessary dissemination of Top Secret information.

2. Release to a subordinate echelon only the absolute minimum of Top Secret information necessary for proper planning or action.

3. Transmit Top Secret information within the command by direct personal contact.

4. Maintain a continuous chain of receipts for Top Secret material.

5. Maintain a current roster of persons within the command who are cleared for access to Top Secret information.

Certain commands within the Naval Establishment are designated to maintain a Special Security Officer (SSO). The Special Security Officer and all persons detailed to assist this person are granted a special clearance by the designator.

Material intended for the Special Security Officer is wrapped in a double-sealed opaque envelope. The outer container bears the command address. The inner container bears the command address, the classification of the material, and the notation "To be Opened only by the Special Security Officer." Packages so marked are immediately delivered, with the

inner container unopened, to the Special Security Officer. If the receiving command does not have a Special Security Officer, the inner container is not opened and will be marked "No Special Security Officer at this Command." The inner envelope is placed in an outer opaque envelope and returned to the sender via the Armed Forces Courier Service.

Additional information concerning security is included in the Department of the Navy Information Security Program Regulation, OPNAV Instruction 5510.1 series.