DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
914 CHARLES MORRIS CT SE
WASHINGTON NAVY YARD DC 20398-5540

REFER TO:

COMSCINST 5530.4A
N1
8 January 2004

COMSC INSTRUCTION 5530.4A

Subj: MSC HEADQUARTERS FORCE PROTECTION/PHYSICAL SECURITY PLAN

Ref: (a) OPNAVINST 5530.14C
(b) NDWINST 5530.14A
(c) SECNAVINST 5510.36
(d) SECNAVINST 5510.30A
(e) OPNAVINST 5239.1B
(f) COMSCINST 3440.3H
(g) COMSCINST 4400.4C
(h) COMSCINST 7321.1B

1. Purpose. To provide guidelines and procedures for implementing force protection measures at Headquarters, Military Sealift Command (MSC) and to define specific actions required to safeguard personnel, equipment (including Automated Information Systems [AIS] assets), facilities, material, and documents from unauthorized access such as espionage, sabotage, theft, or other unlawful acts. This instruction is a complete revision and should be read in its entirety.

2. Cancellation. COMSCINSTs 5530.4 and 5522.1A.

3. Mission. The mission of MSC is to meet Department of Defense (DOD) requirements by providing efficient sea transportation, combat-ready logistics forces, and reliable special mission ships in peace and war.

4. Responsibilities. Commander, MSC (COMSC) is responsible for ensuring that appropriate measures are taken to safeguard personnel and property within the command; establishing and maintaining a formal force protection program, and acting as final authority in determining the type and extent of force protection required for the facility.

5. Applicability. This instruction is applicable to all military and civilian personnel assigned to or employed/located at Headquarters MSC.

//S//
JOHN B. STROTT
Chief of Staff

Distribution:
COMSCINST 5215.5
List I (Case A, B, C)

TABLE OF CONTENTS

Chapter 1 - Security Office Staffing and Functions

Chapter 2 - Security Measures

Chapter 3 - Control Measures

Chapter 4 - Material Control

Chapter 5 - Force Protection Aids

Chapter 6 - Security Force

Chapter 7 - Force Protection Conditions (FPCONs)

APPENDICES

CHAPTER 1

SECURITY OFFICE STAFFING AND FUNCTIONS

1-1 STAFFING

Director, Military Personnel and Security Division (N15) serves as the Security Officer at Military Sealift Command (MSC) and comes under the cognizance of the Director, Maritime Forces and Manpower Management (N1). The MSC Security Officer is responsible for supervising two security specialists, GS-080-5 through 12, who implement the command's Force Protection Plan. The security specialists work as a team in performing duties in personnel, information, and force protection while maintaining liaison with various Naval, DOD, and non-DOD activities.

1-2 SECURITY OFFICER

The Security Officer, either personally or through subordinates, is responsible for the following:

a. Implementing, administering, training, and overseeing a comprehensive security program consistent with command guidelines and those established by higher authority. Serving as the command representative for security matters.

b. Designing and developing protection systems and devices to ensure that the material and facilities are not compromised, sabotaged, subjected to malicious mischief, or other forms of willful interference.

c. Identifying restricted areas, setting up personnel access systems; developing procedures for the movement, and handling of classified and other sensitive materials.

d. Preparing correspondence, reports, and directives.

e. Formulating emergency plans; maintaining liaison and personal contact with Information Systems Security Manager (ISSM), Federal agents, and Naval District Washington (NDW) Security Department.

f. Accomplishing other related duties as specified in reference (a).

1-3 SECURITY CLERK/SECURITY SPECIALIST

The security specialists work independently under the supervision of the MSC Security Officer in performing the following duties:

a. Develop and enter data in buildings 210 and 157 computerized access systems.

b. Conduct force protection surveys for buildings 210 and 157.

c. Supervise random security inspections.

d. Oversee and/or assist in emergency evacuations, as required, in buildings 210 and/or 157.

e. Supervise and provide guidance to contract Security Guard personnel in buildings 210 and 157.

f. Maintain an inventory of all command security containers. Also, ensure that cipher locks and security containers are changed by authorized personnel.

g. Maintain liaison with the NDW Security Officer regarding various security policies, security-related incidents and activities.

h. Provide authorization letters/memoranda to employees for an NDW security badge. Provide authorization letters/memoranda to NDW Security after receipt of visit request and written approval from MSC sponsor.

i. Produce and maintain buildings 210 and 157 contract guard force post orders.

j. Oversee the command Intrusion Detection Systems (located on the 1st floor, 210), and exits in building 210 or 157. Monitor closed circuit TV and recording of information.

CHAPTER 2

SECURITY MEASURES

2-1 RESPONSIBILITIES

a. Security Officer. The Security Officer is responsible for planning, coordinating and supervising the command's Force Protection Program. Included in the program are the following:

(1) All matters pertaining to force protection.

(2) Formulating Emergency Plans.

(3) Reviewing and updating the COMSC Force Protection Plan.

(4) Complying with other related duties as specified in reference (a).

(5) Establishing and maintaining liaison with personnel or agencies to ensure timely and organized support in event of an emergency.

b. MSC military personnel and civilian employees will be responsible for adhering to the sound security practices set forth in this plan and become familiar with evacuation procedures used during all emergency situations.

2-2 MATERIAL CONTROL

a. General. MSC Physical Security and Loss Prevention Program is designed to safeguard resources from theft, vandalism, or misappropriation by establishing an unacceptable risk of detection and/or apprehension. References (a) and (b) provide more detailed guidance.

(1) Accountability. Personnel taking government equipment (i.e., laptop computers, typewriters, recorders, etc.) out of buildings 210 and 157 will, upon exiting the building, have equipment scanned by the Security Guards and thereby entered into the Front Desk database or equipment log, as appropriate. Upon entering the building, the property will be scanned to ensure there is a record. Excess property/equipment leaving the building must have a property pass from a designated Logistics Directorate (N4) representative or a letter of authorization signed by a designated Command, Control,

Communication and Computer Systems (C4S) Directorate (N6) representative. Memoranda and property passes will be in duplicate; the original to be retained on file and the duplicate to be retained by the bearer. Buildings 210 and 157 Security Guard post orders identify the designated N6 personnel authorized to sign the letter of authorization.

(2) Reporting Losses. Loss of government or personal property should be reported immediately to the MSC Security Officer who will notify NDW Security Department. NDW Security will contact the NDW Regional Investigations who will notify the Naval Criminal Investigative Command (NCIS). NDW Regional Investigations will be the primary resource for detection and investigation of lost, stolen or missing government property. All government property, regardless of value or classification will be reported to this agency for stolen or recovered property.

(3) Administrative Inspections. Commander, Military Sealift Command (COMSC) is responsible for readiness, security, health, welfare, and safety of members of this command and those members of other commands who use MSC property. A sign will be posted in buildings 210 and 157 advising that all handcarried items, such as briefcases, bags, boxes, etc., will be subject to random security inspections prior to entrance or departure. The inspections will be directed by COMSC and the procedures listed below will be followed:

(a) The inspection shall be specifically authorized in writing by COMSC or his/her designee. Appendix C provides a sample authorization letter.

(b) Personnel will be stopped randomly without regard to status (i.e., civilian employees, contractor, military personnel or visitors). Individuals will be selected with a random numbering system outlined by the Commander or designee's signed authorization.

(c) Security Guards will explain to the personnel stopped that an inspection is being conducted. The individual will be asked to step out of the walkway and to open his/her briefcase, purse, etc. for inspection. If an individual entering refuses to do this, he or she will be prohibited from entering the spaces and no inspection will be conducted. For those leaving, the inspection will still be done even after objection of the party and, if necessary, the Security Officer will notify NDW Security Department. Otherwise, the individual will be allowed to proceed after inspection.

b. Physical Security Review Committee (PSRC)

(1) General. COMSC has overall responsibility for force protection and law enforcement matters affecting MSC buildings 210 and 157. COMSC will establish the PSRC which will include the Chief of Staff (N02) as chairperson.

(2) The PSRC will meet in accordance with reference (a) and perform the following:

(a) Assist in determining force protection requirements for and evaluating security areas at MSC.

(b) Advise on establishment of restricted areas.

(c) Review reports of significant losses or breaches of security and recommend improvements to the Physical Security and Loss Prevention Program.

(3) The PSRC membership will include the following staff members but not limited to additional representatives so determined by the Commander:

(a) Chief of Staff (N02) (Chairperson)

(b) Security Officer (N15)

(c) Maritime Forces and Manpower Management Director (N1)

(d) Logistics Director (N4)

(e) Facilities Officer

(f) Information Systems Security Manager (ISSM) (N61)

(g) Comptroller (N8)

c. Security Officer. Under the direction of COMSC, the Security Officer is responsible for the establishment, administration, and coordination of force protection and law enforcement measures involving the protection of military personnel, civilian employees, and MSC visitors.

d. Program Managers/Functional Directors/Special Assistants. Each Program Manager/Functional Director/Special Assistant is responsible for the security of personal property, equipment, and spaces assigned to that office or members of that office. Program Managers/Functional Directors/Special Assistants will maintain close liaison with the MSC Security Officer regarding Physical Security and Loss Prevention and ensure proper compliance with the command's program.

2-3 INTERNAL CLASSIFIED DOCUMENT CONTROL PROCEDURES

a. Security Manager. The Security Manager is responsible for planning, coordinating and supervising the Information and Personnel Security Program.

b. Control Information. Effective control of DOD information will be maintained at all times in accordance with reference (c). All classified material received at MSC must be brought into the mailroom accountability system. **SECRET** or **CONFIDENTIAL** classified material received through the mail or any other means of transmission will immediately be handcarried to the mailroom for entry into the classified material accountability system. **TOP SECRET** or **CMS** classified material received by mail or any other means of transmission will immediately be handcarried to the Top Secret (TS) Classified Material Control Officer and CMS Custodian who is assigned to the C4S Director (N6). **TOP SECRET** or **NATO** classified material is not handled by mailroom personnel or entered into the mailroom classified material accountability system.

c. Storage. All classified documents, when not in use, will be stored in a GSA-approved security container. MSC Security will maintain an inventory of all security containers, the locations, custodians, and record of combination changes.

(1) Combinations to the security containers must be changed when an individual knowing the combination no longer requires access, when the combination has been subject to possible compromise or when the security container has been discovered unlocked or unattended, when the container is first put into service or when the security container has been taken out of service. Cipher lock combinations will be changed when an individual knowing combination no longer requires access or when the combination has been subject to possible compromise.

(2) Combination changing tools are maintained by the MSC Security Office and are available for use by authorized MSC employees to change combinations to MSC security containers. The custodian must advise the MSC Security Officer when one of the above listed occurrences have come into effect and at that time set up an appointment with an MSC security specialist for changing the combination. When scheduling the appointment, ensure that the custodian of the security container is present and available during the combination change.

(3) Combinations are not to be changed by individual employees unless approved by the MSC Security Officer in advance.

(4) Security containers will be repaired by an approved and authorized locksmith who has been granted a government security clearance at the level of the classified material in the container. The company for which he or she works must also have a facility security clearance at that level. Repair requests will be approved by the MSC Security Officer and coordinated with N4.

d. Destruction. Classified documents that are no longer required will be immediately destroyed by using a GSA-approved shredding machine located in buildings 210 and 157, returned to the MSC mailroom, or put in burn bags for N6 burn runs. Locations of shredding machines are as following:

(1) **Building 210**

- Room 490
- Room 435
- Room 375-1
- Room 365
- Room 355
- Room 282
- Room 235
- Room 170
- Room 105

(2) **Building 157**

- Room 225
- First Floor (hallway to PM1 spaces)

e. Emergency Removal. MSC shall develop an emergency plan to protect classified material in a manner that will minimize the risk of injury or loss to personnel. If removal of classified material from building 210 or 157 is not feasible, the material shall be stored in a GSA-approved container. Appendix B provides an MSC Emergency Destruction Plan.

2-4 PERSONNEL IDENTIFICATION REQUIREMENTS

a. Because buildings 210 and 157 are restricted areas, one of the following forms of identification badges are approved before unescorted entrance to the buildings:

(1) NDW MSC badge.

(2) National Capital Region (NCR)/Pentagon (PNT) badge with pink, red and/or white backgrounds.

(3) MSCLANT Norfolk Virginia, MSCPAC San Diego California, MSCFE Yokohama Japan, MSCEUR Naples Italy, APMC Virginia Beach, Virginia or MSCCENT Bahrain.

(4) United States Transportation Command (USTRANSCOM).

(5) Active Duty (Identification card).

b. Personnel requesting entry to buildings 210 and 157 to perform maintenance or contract services will be positively identified prior to allowing entry. A current Visit Request must be on file in the MSC Security Office for those individuals in order to be listed in the computer access system. The Visit Request can be either a letter from the agency/company on agency/company letterhead or a form listing the individual's full name (last name and first name), social security number, date and place of birth, citizenship, purpose of visit, name of MSC point of contact, and length of visit (not to exceed 1 year). The correspondence must be signed by a security representative or a designated agency representative.

c. Individuals who request entry and cannot produce required identification media, and/or are not on the access list, will be denied entry until they are personally escorted/ accompanied by a staff member when in buildings 210 and 157.

2-5 PERSONNEL SECURITY CLEARANCE AND ACCESS REQUIREMENTS

Before contractors and visitors at MSC are granted access to classified information, clearance eligibility must be verified by the MSC Security Officer. Contractors and visitors must ensure that a Visit Request is forwarded by mail or fax to the MSC Security Office prior to their visit. Visit Requests will not be accepted if hand delivered by an individual whose name is on the Visit Request. The information provided in the Visit Request must be in compliance with reference (d). Clearance eligibility on employees will be verified by MSC through the Department of the Navy (DON) Central Adjudication Facility JPAS, DCII or Human Resources Office (HRO) record center. A security clearance access list is provided to Program Managers/Functional Directors/Special Assistants at least monthly and at that time supervisors will review and make requests for changes as required.

2-6 BARRICADED CAPTOR/HOSTAGE SITUATIONS

MSC will comply with the procedures delineated in reference (f) concerning these situations, as applicable.

2-7 FORCE PROTECTION CONDITIONS

MSC shall comply with applicable threat requirements outlined in reference (b).

2-8 BOMB THREAT/DETECTION PROCEDURES

Personnel will comply with procedures outlined in reference (f).

2-9 EMERGENCY EVACUATION

In the event of fire, comply with the procedures outlined in reference (f).

2-10 DESTRUCTIVE WEATHER

MSC will follow local NDW procedures when destructive weather threatens or when snow emergency procedures go in effect.

2-11 KEY AND LOCK CONTROL

a. Responsibilities

(1) Commander. Responsible for establishment of a key control program within the command and appointment of a key control custodian.

(2) Key Control Custodian. Responsible for the command's overall key control program as outlined in reference (a). Keys to the command Restricted Areas are maintained in locked key cabinets and security containers located in the MSC Security Office. The Key Control Custodian is required to perform spot checks and inventory all keys at least quarterly.

(3) Program Managers/Functional Directors/Special Assistants. Responsible for ensuring that the key control program is implemented within their codes. He/she must notify N15 in writing when an employee departs the command before returning keys. Program Managers/Functional Directors/Special Assistants will request duplication of keys through N15.

b. Key Control Log

(1) A Key Control Log will be maintained with each key locker and when not in use will be kept under constant control by the custodian. When no personnel are available to oversee the log, it will be secured in an area qualified to hold classified material. The log will contain information to include keys issued, to whom, date/time issued and returned and the signature of the person drawing or returning the key. The control log will be checked against the key at the end of each watch or work period to account for all keys and an appropriate notation will be made in the Command Duty Log. They are located in the Command Center (CC), which is manned 24 hours a day, and the Security Office, which is a secure office. None of these keys are reissued.

(2) Included within the key inventory are all keys, locks, padlocks, and locking devices used to protect or secure restricted areas and activity perimeters, critical assets, classified material, and sensitive materials and supplies. Not included in the inventory are keys, locks, and padlocks for convenience, privacy, and administrative or personal use.

(3) There will be at least two duplicate/spare keys kept on hand. Duplicates will at no time be checked out to personnel for convenience. Before a duplicate key is checked out, the key custodian will establish the need for the duplicate and the disposition of the original. All requirements for duplicate keys will be routed through the key custodian to the command security office. A record of keys replaced will be kept in the key control log for future reference and review.

c. After Hours Procedures. Keys are maintained in the CC. The Staff Duty Officer (SDO) has custody of the keys, which can be used to access all spaces (non-restricted including maintenance and restricted areas in buildings 210/157). Each of the keys are labeled and a log is maintained by the SDO who will use these keys for the duty sections to make the security checks for buildings 210 and 157 daily.

2-12 SECURITY CONTAINER

a. Classified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in a locked GSA-approved security container.

b. Security container combinations will be maintained by the MSC Security Officer in a security container and treated at the highest level of the information stored in it. Custodians for security containers will be responsible for ensuring combinations are changed when put in service, when persons who know the combination no longer require access, when taken out of service; if found unsecured, unattended, or shows evidence of unauthorized entry attempt. A Standard Form (SF) 700 will be completed with custodian names and the combination, which will be recorded and put in the envelope portion of the SF 700. The combination envelope will be stamped with the highest classification of the information in the container.

c. When the security container is opened and closed, the action will be recorded on an SF 702. At the end of the day, containers will be checked and the check recorded by the last person in the office. Each Program Manager/Functional Director/Special Assistant will be responsible for the checks in their spaces with the final check of the spaces with an SF 701. An SF 701 is required for each space where there is a security container.

2-13 CIPHER LOCK/HANDKEY

Combinations to cipher locks will be changed at least every 6 months and when persons who know the combination no longer require access or when there is evidence of an unauthorized attempt or access. Combinations to the spaces can also be recorded on the SF 700 but not required.

2-14 PROTECTIVE LIGHTING

Continuous lighting at both entrances to buildings 210 and 157 illuminates the vehicle parking area and provides assistance to the NDW Security Police in preventing illegal intrusion attempts.

2-15 COMMUNICATIONS

Classified information will not be discussed over non-secure telephones or in non-secure spaces.

2-16 INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

The ISSM will ensure command ADP equipment is operated in accordance with reference (e).

CHAPTER 3

CONTROL MEASURES

3-1 CONTROL MEASURES (RESTRICTED AREA)

This chapter identifies all mission essential areas within MSC. Buildings 210 and 157 are designated as a restricted area. All persons are forbidden to enter established restricted areas unless their official duties require such entry. As a restricted area, there are procedures for conducting administrative inspections of persons entering and leaving such areas. The purpose is to detect/prevent the introduction of prohibited items (firearms, explosives, drugs, etc.) and to detect/prevent unauthorized removal of government property/material. Administrative inspections should be conducted on a random basis daily, but at least monthly. The inspections shall be specifically authorized in writing by COMSC or his/her designate, the MSC Security Officer. Security Guards will conduct the inspections with a member of the MSC Security Office or NCIS office representative present and in charge during the inspections.

3-2 AREA SECURITY

Areas, offices and other structures at MSC which are designated as restricted fall into one of the following categories:

a. Level Three Areas. A Level Three restricted area is the most secure type of restricted area. It may be within less secure types of restricted areas. Entrance procedures for all Level Three restricted areas include an access list of personnel authorized to enter area without an escort. The access list will include name and rate/rank of each individual permitted uncontrolled access. Requirements for Level Three areas are as follows:

(1) Personnel identification and control system (i.e., activity area pass/ID or military/civilian government identification card) must be displayed at all times on the outer garment. During normal duty hours, use of an access list and entry/departure log is required. After normal duty hours, all personnel accessing the area must be logged in/ out.

(2) Only persons whose duties require access and who have been granted appropriate security authorization would be admitted to Level Three areas. Persons who have not been cleared for access to the security interest contained with a Level Three area may be admitted, but they must be controlled by an escort, and the security interest protected from compromise or other degradation.

(3) When secured, a check will be made at least twice every 8-hour shift or, if adequately equipped with an operational IDS, once per 8-hour shift, for signs of unauthorized entry or other activity, which threatens to degrade security of the Level Three restricted areas.

b. Level Two Areas. Buildings 210 and 157 have no Level Two areas.

c. Level One Areas

(1) Persons authorized to enter Level One area are those assigned duties requiring their presence while actively engaged in performing such duties.

(2) A Level One restricted area is the least secure type of restricted area and serves as a buffer zone for Levels Three and Two restricted areas providing administrative control. The following minimum-security measures are required for all Level One restricted areas.

(a) A personnel identification and control system.

(b) Ingress and egress controlled by guards or other appropriately trained personnel.

(c) Procedures to control entry into the area by individuals (military, civil service, contractors, official business, individuals who render a service [e.g., vendors, delivery people, designated contractors performing a service, etc.]) retired military, and unofficial visitors.

d. Non-Restricted Areas. A non-restricted area is an area which is under the jurisdiction of MSC but to which access is minimally controlled or uncontrolled. Such an area may be open to uncontrolled movement of the entire command or the area can be enclosed by a checkpoint, which would ensure access for official business or other authorized purpose only. Non-restricted areas will not be located inside restricted areas. All areas not designated as Restricted Areas are designated as non-restricted areas at MSC.

e. Posting of Restricted Areas. Restricted areas within MSC buildings will be posted simply as “Restricted Area.” Posting of signs will be in accordance with Appendix 9 of reference (a).

f. Movement Control within Security Areas. Security personnel will have full cooperation and participation of other military and civilian personnel. All personnel in security areas will be instructed to consider each unidentified or improperly identified individual as a trespasser and report him/her to their supervisor, the Security Officer or to other appropriate authority.

g. Personnel Identification and Control Procedures. Buildings 210 and 157 are restricted areas; therefore, entry will be granted only to authorized personnel. Security Guards will verify the identity of all personnel before entry to MSC buildings 210 and 157. Personnel must provide a current picture badge and/or be on the automated access control system before entry. Personnel and visitors will comply with procedures as described below.

(1) MSC military and civilian employees with the following authorized badges are not required to sign in the logbook.

(a) NDW MSC badge or MSC badge.

(b) NCR/PNT badge (pink, red, and/or white).

(c) MSC Area Command picture badges.

(1) MSCLANT Norfolk, Virginia

(2) APMC, Virginia Beach, Virginia

(3) MSCPAC San Diego, California

(4) MSCFE Yokohama, Japan

(5) MSCEUR Naples, Italy

(6) MSCCENT Bahrain

(2) Visitors in the Armed Forces of the United States (military identification cards – green, red, or blue colored or Common Access Cards) who are entered in the access database are authorized access to buildings 210 and 157 but must sign in the access database. Exceptions to this rule are also listed below.

(a) Reservists who are not in access control system must be escorted. (This does not include command suite visitors.)

(b) Active duty military who are not on the access must present their active duty ID to the Security Guard and sign in.

(c) Military, civilian or visitors who are on access system will be provided the following internal badges prior to verifying their identity. Individuals must sign in/out visitor log prior to being provided a badge.

(1) "T" badge will be given military or civilian employees who forget their MSC picture or NCR/PNT badge.

(2) "V" badge will be given to active duty military, Federal Government visitors or contractors.

(3) All other visitors who are not on the MSC access system will be given a "Visitor with Escort" badge and those visitors must be escorted at all times. The Security Guard will also contact the point of contact to request an escort for the visitor.

(4) Command Suite/VIP Visitors. The Security Guard will be notified before any visits to the command suite (N00, N01, and N02). Visitors will be escorted by someone in the command suite. No sign-in logbook is required. The following procedures will be followed:

(a) Security Guard will be notified by the command suite representative (Flag Secretary, Flag Lieutenant, or Flag Writer, etc.) prior to any visits to the command suite.

(b) Security Guard will contact the command suite when visitor(s) arrives.

(c) Visitor(s) will be escorted by someone in the command suite.

(d) Visitor(s) will not be required to show identification, the escort from the command suite will verify identity of visitor(s).

(5) Weekend Drilling Reservists. U.S. Naval Reservists, who perform weekend drills and meet at COMSC Headquarters, will ensure that a list is provided periodically to the MSC Security Office prior to their visit. The following procedures will be followed by the Security Guards in buildings 210 and 157.

(a) Check the military identification of the reservist.

(b) Check the access system to find the individual's name.

(c) Ensure that reservist signs in/out log.

(d) If the name is in the access system and the reservist holds an MSC badge, they are not required to be issued a “V,” “T,” or “Visitor with Escort” badge.

(e) If name is not in access system, issue reservist a “V” badge.

(6) Law Enforcement. The Security Guards shall cooperate with Federal, State, county, and local law enforcement officials who visit MSC in an official capacity. The official will present their credentials to the Security Guard and after verification of their identity MSC security office will be notified immediately during regular working hours or the SDO after hours and on weekends and holidays.

(7) Agents of Investigative Agencies. For all Federal Bureau of Investigation (FBI), Naval Criminal Investigative Service (NCIS), Defense Investigative Service (DIS), U.S. Treasury Department, Secret Service, or Office of Personnel Management (OPM) investigative personnel requesting admittance to building 210 or 157, the procedures below will be followed:

(a) Credentials will be checked.

(b) MSC Security Office will be notified during normal hours; after hours, the SDO will be notified.

CHAPTER 4

MATERIAL CONTROL

4-1 PROPERTY CONTROL PROCEDURES

References (g) and (h) require the controlled movement of government property. The use of property passes is essential to external security and loss prevention. Every precaution must be exercised to ensure the integrity of government material.

a. Property Pass (NAVSUP 155). This form authorizes removal of certain specifically described government or private property from MSC through control points. It is the standard form to be used by MSC when appropriate documentation showing proof of ownership or authorization for possession is not with the government or private property. Other proof of ownership or authorized documentation is:

(1) Government bills of lading.

(2) Commercial bills of lading.

(3) Adding machine tape annotated "SERVMART COMSC" used for all SERVMART purchases.

(4) DOD Single Line Item Release/Receipt Document (DD Form 1348-1).

(5) Requisition and Invoice/Shipping Document (DD Form 1149).

(6) Blanket Purchase Authorization (BPA) (NSC 4225/1).

(7) Subsistence Report Multi-use (NAVSUP 1059).

(8) Material Inspection and Receiving Report (DD 250).

b. Property Passes

(1) A property pass, issued by N4, will accompany government property from MSC through buildings 210 and 157 guard force.

(2) Property passes will be picked up by the guard force in either building 210 or 157.

(3) The guard force/security official will review the property pass for authenticity of the signature or entries for documentation or where serial numbers are not annotated on the property pass.

c. N6 Laptop Pool Form.

4-2 RESPONSIBILITIES

a. The Logistics Director (N4) shall:

(1) Maintain accountability and control over MSC property passes.

(2) Obtain an adequate on-hand supply of property passes and ensure that they are stored in combination lock containers.

(3) Appoint a directorate custodian to obtain and maintain accountability of property passbooks (including disposition of originals) and return completed passbooks to the Security Officer. Information regarding any suspected usage irregularities in property passes shall be reported to the Security Officer.

(4) List items/property being removed from buildings 210 and/or 157 and record serial numbers for each item on property pass. Also record dates of issue, signatures, and duty stations of persons to whom issued and keep for control purposes.

b. The Director, C4 Systems (N6) shall:

(1) Initiate disposition of all ADP equipment.

(2) Determine if items will be reissued or disposed of as excess/surplus property.

(3) Sign as new subcustodian for items retained, and N43 will sign as new subcustodian for items to be turned in for disposal.

c. The Security Officer shall:

(1) Review MSC property passes returned. Send copy to Property Manager (N43a) to update property control system.

(2) Inspect completed passbooks received from N4 to ensure all returned passes have been matched with the duplicate copy and each missing original has been accounted for by the issuing directorate. Investigate all matters indicating possible misuse, fraudulent changes, or any other irregularities. Program Managers/Functional Directors/ Special Assistants and N4 will be advised of any discrepancies and will be requested to take corrective action.

(3) Periodically review the use and application of property passes and ensures they are being properly utilized.

(4) Establish and maintain liaison between NDW Security and other appropriate officials to ensure property passes issued by MSC are returned to this command.

4-3 INFORMATION MATERIAL CONTROL

Control of classified and Privacy Act information/material is addressed in reference (c). The Security Manager is responsible for the information and personnel security program; the ISSM is responsible for the ISSM security program.

CHAPTER 5

FORCE PROTECTION AIDS

5-1 SECURITY LIGHTING

DOD security personnel are responsible for the inspection of security lighting, while maintenance comes under the jurisdiction of the Public Works Department.

a. Protective Lighting. Protective lighting is utilized around the perimeter areas of buildings 210 and 157 as a means of security illumination for workers entering and departing during hours of darkness.

b. Auxiliary Lighting. Generators and power source will be considered for critical areas. A backup generator is located on the roof of building 210 for power.

5-2 POWER FAILURE PROCEDURES

a. In the event of a commercial power failure during regular work hours, NDW Public Works Department will be notified by COMSC (N4) and the building 210/157 Security Guards will be notified.

b. After regular work hours, NDW Security Department and NDW Public Works Department will be notified by building 210 Security Guard or by the MSC SDO.

5-3 INTRUSION DETECTION SYSTEM (IDS)

a. IDS is designed to detect, not prevent actual or attempted penetrations. IDS contributes to the overall force protection posture and the attainment of security objectives. The IDS systems are located at entrances and exits of buildings 210 and 157. When the IDS system alarm goes of, the contract Security Guards in building 210 will respond by calling the MSC Security Officer during normal work hours and after hours by calling NDW Security Police and/or the MSC SDO. In the event of power failure, the Security Guard will notify the SDO who will check the exits in buildings 210 and 157 to determine if there was a successful attempt to gain entry to MSC spaces. CCTV is located around the perimeter of buildings 210 and 157. The Security Guard in building 210 will monitor the cameras while video taping is conducted in the MSC Security Office.

b. The following personnel at MSC are responsible for ensuring that the IDS is maintained.

(1) COMSC has overall responsibility for the proper installation and hook-up of all alarms in buildings 210 and 157 including the designated spaces/areas.

(2) The Security Officer (N15) and the Logistics Director (N4) must approve all systems prior to hook-up to ensure compatibility and the Director, C4 Systems has overall upkeep, maintenance responsibility for the system.

(3) The MSC Security Officer will provide and monitor the alarm system in MSC buildings 210 and 157.

(4) N6 is responsible for ensuring maintenance of CCTV and IDS equipment connected to the Johnson Controls Metasy System.

CHAPTER 6

SECURITY FORCE

6-1 GENERAL

Standard operating procedures will be provided at the Security Guard post in buildings 210 and 157. Each contract Security Guard assigned to the post in buildings 210 and 157 will become familiar with the special orders, which cover specific situations pertaining to that post. Each Security Guard reporting for duty will immediately review the post orders and become familiar with its contents at the beginning of his/her watch. At the end of each watch, the Security Guard will print out a security badge inventory, provide an end-of-shift entry to the log book and brief the oncoming Security Guard of any changes to the post orders or any significant special incidents. The guard orders will be reviewed at least semiannually by the MSC Security Officer.

6-2 RESPONSIBILITIES

The armed Security Guards at MSC Headquarters are located at the entrances of buildings 210 and 157 and will perform the following duties at the above listed posts:

a. Control the entry and exit of all personnel, equipment, and property.

b. Protect U.S. Government property and employees and visitors.

c. Maintain all of the guard logs/registers in a neat and legible manner.

d. Keep constantly alert and observe everything within sight or hearing.

e. Report all violations of published and/or verbal orders.

f. Remain on assignment until properly relieved by direction of contract guard supervisor.

g. Pass all information relative to assignment to the relieving guard.

h. Turn over any money or valuables recovered to the MSC Security Officer.

i. Endeavor to prevent theft, pilferage, riots, espionage, sabotage, and other criminal acts.

j. Ensure that all personnel bringing and removing government and/or agency property have a valid property pass (if necessary) and/or sign the property log book upon entering building 210/157.

k. Ensure that prohibited material such as firearms, explosives, drugs, etc. does not enter the building except law enforcement officers.

l. Issue appropriate “V,” “T,” or “Visitor with Escort” badges to visitors or employees. Ensure that none of these badges leave buildings 210 and 157.

m. Be professional and courteous in all situations.

n. Guards may apprehend and detain persons only within their jurisdiction and then only for as long as necessary to transfer such persons to law enforcement personnel.

6-3 SUPERVISION OF ASSIGNED SECURITY GUARDS

Supervision of the assigned Security Guards will comply with the clauses and provisions of the contract the Navy has with the security contractor concerning supervision.

6-4 METHODS OF FORCE AND PRECAUTIONS FOR USE OF DEADLY FORCE

Assigned Security Guards will comply with the clauses and provisions in their employer’s contract with the Navy concerning firearms safety, use of minimum force, use of deadly force and methods of force. In addition, assigned Security Guards will comply with the deadly force guidance and procedures in DOD Directive 5210.56 of 1 November 2001 to the extent that the directive is more restrictive concerning use of force than the contract.

6-5 EMERGENCY PROCEDURES

a. During emergencies (fire alarm, medical emergency, evacuation, etc.), emergency personnel will be permitted immediate entry. Contract Security Guard will immediately call the MSC Security Officer during normal hours or the SDO, if after normal work hours, weekends and/or holidays, and advise them of the situation.

b. In case of fire or natural disaster, the Security Guard in building 210 or 157 will immediately notify the following as applicable:

➢ **Fire Department——433-3333**	➢ **Ambulance—433-3269**	➢ **SDO—685-5155 (1630 - 0600)**
➢ **NDW Security Dept—433-2411/3018**	➢ **MSC Security Officer—685-5128/5144/5145 (0600 - 1630)**	

CHAPTER 7

FORCE PROTECTION CONDITIONS (FPCONS)

7-1 INTRODUCTION

Information and warnings of terrorist activity against MSC and attached personnel will normally be received from security authorities or through security agencies. Information may come from NDW Police Department, be received directly by command or agency as a threat or warning from a terrorist organization or be in the form of an attack. Reference (f) provides specific guidelines for emergency evacuation of personnel for buildings 210 and 157.

7-2 DECLARATION OF FPCONs AND MEASURES FOR IMPLEMENTATION

The declaration of FPCONs and implementation of measures may be decreed by COMSC, following receipt of intelligence through official sources, NDW, other official channels or following an anonymous threat message. Actions should be based on all appropriate sources of information to include intelligence, law enforcement, and knowledge of the location situation. Reference (g) provides detailed FPCON procedures.

7-3 THREAT ASSESSMENT GUIDELINES

a. General Guidelines. The following general guidelines provide for uniform implementation of security alert conditions. Assessment factors are defined as follows:

(1) Existence. A terrorist group is present, or able to gain access to a given building.

(2) Capability. The acquired, assessed or demonstrated level of capability to conduct terrorist attacks.

(3) Intentions. Recent demonstrated anti-U.S. terrorist activity or assessed intent to conduct such activity.

(4) Targeting. Current credible information on activities indicative of preparations for specific terrorist operations.

(5) Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

b. Threat Levels. Threat levels are based on the degree to which combinations of the following factors are present:

(1) Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history, and intentions must be present.

(3) Medium. Factors of existence, capability, history, and must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and/or capability may or may not be present.

7-4 VULNERABILITIES

The following are MSC vulnerabilities:

a. Communication lines and support facilities.

b. Power supply transmission (primary and alternate).

c. Logistic and storage facilities.

d. Computer facilities - access to LAN or individual standalone microcomputers.

e. Intrusion detection system monitor station.

f. Water sources.

g. Access control system.

h. Personnel -

(1) Flag officers/senior civilians.

(2) Foreign personnel assigned to or visiting the command.

7-5 FORCE PROTECTION CONDITIONS

a. FPCON ALPHA. This condition is declared as a general warning of possible terrorist activity, the nature and extent of which is unpredictable, when the circumstances do not justify full implementation of the measures of FPCON BRAVO. However, it may be necessary to implement selected measures from FPCON BRAVO. The measures in this FPCON must be capable of being maintained indefinitely.

b. FPCON BRAVO. This condition is declared when there is an increased and more predictable threat of terrorist activity even though no particular target is identified. The measures of this FPCON must be capable of being maintained for weeks without causing undue hardship, without affecting operational capability and without aggravating relations with local authorities.

c. FPCON CHARLIE. When an incident occurs or when intelligence is received indicating that some form of terrorist action against installations or personnel is imminent. Implementation of this measure for more than short periods will probably create hardship and will affect peacetime activities of the installation and its personnel.

d. FPCON DELTA. A terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally this FPCON is declared as a localized warning.

APPENDIX A

SECURITY SERVICING AGREEMENT

NOTE: MSC Security Servicing Agreement will be separate from the MSC Force Protection Plan.

APPENDIX B

EMERGENCY DESTRUCTION PLAN

This Emergency Destruction Plan provides for the protection of classified material in a way that will minimize the risk of personal injury or loss of life. Because MSC buildings 210 and 157 are restricted, force protection measures have been put into place to minimize the risk of loss of compromise of classified information in an emergency situation. Additionally, the force protection procedures in place will supplement the protection required. MSC's risk posture is assessed as low as a result of the security procedures in place. In the event of an emergency situation, one of the following will designate that an emergency situation exists:

- Commander
- Vice Commander
- Chief of Staff
- Executive Director
- Security Officer
- Operations Officer
- Staff Duty Officer

Program Managers/Functional Directors/Special Assistants are responsible for initiating the destruction of classified material within their directorate. He or she shall identify personnel who will be responsible for the destruction of classified material in an emergency situation.

In order to accomplish an emergency destruction, preplanning must be accomplished. Classified material shall be destroyed in the order of the priority. Priority One--Top Secret; Priority Two—Secret; and Priority Three—Confidential material. Classified material shall be destroyed in DOD approved or an approved National Security Agency (NSA) shredder within buildings 210 and 157. See the listing of locations for each shredder in paragraph 2-3. In order to prepare for an emergency destruction, Program Managers/Functional Directors/Special Assistants shall:

- Destroy all classified material not required.
- Identify the location of all classified documents within the office (e.g., room, safe #, and drawer #).
- Develop an inventory listing for each security container drawer.
- File classified according to priority.
- Limit only one priority to a drawer or set up a system, which will allow everyone to determine priority immediately.
- Mark security containers with priority number (i.e., Priority One, Priority Two, Priority Three) that is florescent.

APPENDIX C

SAMPLE ADMINISTRATIVE INSPECTION AUTHORIZATION LETTER

5530
Ser N15/

From: Commander, Military Sealift Command
To: Building 210 Security Guards

Subj: ADMINISTRATIVE INSPECTION ON 22 APRIL 2003

Ref: (a) COMSCINST 5530.4A

1. Pursuant to my authority and responsibility to determine and ensure the security, military fitness, good order, and discipline of Military Sealift Command (MSC), I hereby direct you to conduct a systematic non-discretionary administrative inspection of personnel entering building 210 on 22 April 2003.

2. You will inspect every 10th person – civilian/military – between 0830 – 1130, at the entrance of building 210.

3. Unlawful weapons, contraband, and other evidence of crime located during the inspection shall be seized.

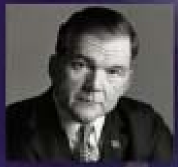
I. M. SECURITY
By direction

APPENDIX D

GUIDANCE FOR PERSONNEL RESIDING OFF-INSTALLATION

"Terrorism forces us to make a choice. We can be afraid. Or we can be ready."

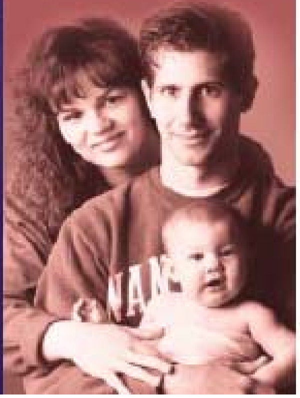
—*Secretary Tom Ridge, U.S. Department of Homeland Security*



www.ready.gov

Preparing makes sense.

The likelihood of you and your family surviving a house fire depends as much on having a working smoke detector and an exit strategy, as on a well-trained fire department. The same is true for surviving a terrorist attack. We must have the tools and plans in place to make it on our own, at least for a period of time, no matter where we are when disaster strikes. Just like having a working smoke detector, preparing for the unexpected makes sense. Get ready now.

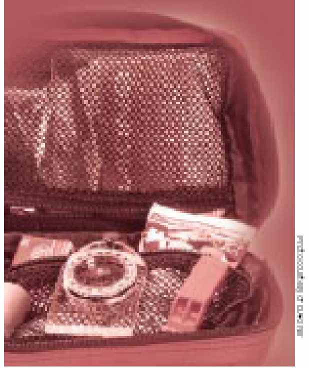


Potential Threats

Terrorists are working to obtain biological, chemical, nuclear and radiological weapons and the threat of an attack is very real. Here at the Department of Homeland Security, throughout the federal government, and at organizations across America we are working hard to strengthen our Nation's security. Whenever possible, we want to stop terrorist attacks before they happen. All Americans should begin a process of learning about potential threats so we are better prepared to react during an attack. While there is no way to predict what will happen, or what your personal circumstances will be, there are simple things you can do now to prepare yourself and your loved ones. Some of the things you can do to prepare for a terrorist attack, such as assembling a supply kit and developing a family communications plan, are the same for both a natural or man-made emergency. However, as you will read below, there are important differences among potential terrorist threats that will impact the decisions you make and the actions you take. With a little planning and common sense, you can be better prepared for the unexpected.

Emergency Supplies

Just like having a working smoke detector in your home, having emergency supply kits will put the tools you may need at your fingertips. Be prepared to improvise and use what you have on hand to make it on your own for at least three days, maybe longer. While there are many things that might make you more comfortable, think first about fresh water, food and clean air. Remember to include, and periodically rotate, medications you take every day such as insulin and heart medicine. Plan to store items in an easy-to-carry bag, such as a shopping bag, backpack or duffle bag. Consider two kits. In one, put everything you will need to stay where you are and make it on your own. The other should be a lightweight, smaller version you can take with you if you have to get away.



Water

Store one gallon of water per person per day for drinking and sanitation in clean plastic containers. If you live in a warm weather climate more water may be necessary.

Food

Store food that won't go bad and does not have to be heated or cooked. Choose foods that your family will eat, including protein or fruit bars, dry cereal or granola, canned foods and juices, peanut butter, dried fruit, nuts, crackers and baby foods. Remember to pack a manual can opener, cups and eating utensils.

Clean Air

Many potential terrorist attacks could send tiny microscopic "junk" into the air. For example, an explosion may release very fine debris that can cause lung damage. A biological attack may release germs that can make you sick if inhaled or absorbed through open cuts. Many of these agents can only hurt you if they get into your body, so think about creating a barrier between yourself and any contamination.

Be prepared to improvise with what you have on hand to protect your nose, mouth, eyes and cuts in your skin. Anything that fits snugly over your nose and mouth, including any dense-weave cotton material, can help filter contaminants in an emergency. It is very important that most of the air you breathe comes through the mask or cloth, not around it. Do whatever you can to make the best fit possible for children. There are also a variety of face masks readily available in hardware stores that are rated based on how small a particle they can filter in an industrial setting.

Given the different types of attacks that could occur, there is not one solution for masking. For instance, simple cloth face masks can filter some of the airborne "junk" or germs you might breathe into your body, but will probably not protect you from chemical gases. Still, something over your nose and mouth in an emergency is better than nothing.

Have heavyweight garbage bags or plastic sheeting, duct tape and scissors in your kit. You can use these things to tape up windows, doors and air vents if you need to seal off a room from outside contamination. Consider precutting and labeling these materials. Anything you can do in advance will save time when it counts.

Basic Supplies

Store a flashlight, battery powered radio, extra batteries, a first aid kit, utility knife, local map, toilet paper, feminine hygiene products, soap, garbage bags and other sanitation supplies, plastic sheeting, duct tape, as well as extra cash and identification. Periodically rotate your extra batteries to be sure they work when you need them.

Warmth

If you live in a cold weather climate, you must think about warmth. It is possible that the power will be out and you will not have heat. Have warm clothing for each family member in your supply kit, including a jacket or coat, long pants, a long sleeve shirt, sturdy shoes, a hat and gloves. Have a sleeping bag or warm blanket for each person.

Special Items

Think about your family's unique needs. Pack diapers, formula, bottles, prescription medications, pet food, comfort items, books, paper, pens, a deck of cards or other forms of entertainment.

Unique Family Needs

□ ______

□ ______

□ ______

□ ______

□ ______

□ ______

□ ______

□ ______

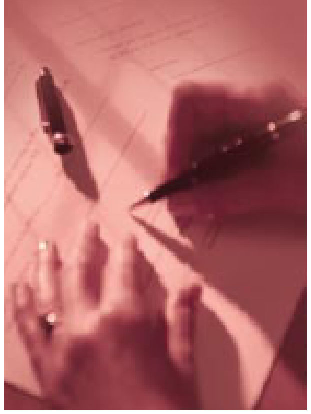
□ ______

□ ______

□ ______

Emergency Planning

You should plan in advance what you will do in an emergency. Be prepared to assess the situation, use common sense and whatever you have on hand to take care of yourself and your loved ones. Think about the places where your family spends time: school, work and other places you frequent. Ask about their emergency plans. Find out how they will communicate with families during an emergency. If they do not have an emergency plan, consider helping develop one.



Develop a Family Communications Plan

Your family may not be together when disaster strikes, so plan how you will contact one another and review what you will do in different situations. Consider a plan where each family member calls, or e-mails, the same friend or relative in the event of an emergency. It may be easier to make a long-distance phone call than to call across town, so an out-of-state contact may be in a better position to communicate among separated family members. Be sure each person knows the phone number and has coins or a prepaid phone card to call the emergency contact. You may have trouble getting through, or the phone system may be down altogether, but be patient.

Deciding to Stay or Go

Depending on your circumstances and the nature of the attack, the first important decision is whether you stay put or get away. You should understand and plan for both possibilities. Use common sense and available information, including what you are learning here, to determine if there is immediate danger.

In any emergency, local authorities may or may not immediately be able to provide information on what is happening and what you should do. However, you should watch TV, listen to the radio or check the Internet often for information or official instructions as it becomes available. If you're specifically told to evacuate or seek medical treatment, do so immediately.

Staying Put and "Shelter-in-Place"

Whether you are at home, work or elsewhere, there may be situations when it's simply best to stay where you are and avoid any uncertainty outside. In fact, there are some circumstances where staying put and creating a barrier between yourself and potentially contaminated air outside, a process known as "shelter-in-place," is a matter of survival. Plan in advance where you will take shelter in this kind of an emergency. Choose an interior room or one with as few windows and doors as possible. Consider precutting plastic sheeting to seal windows, doors and air vents. Each piece should be several inches larger than the space you want to cover so that it lies flat against the wall. Label each piece with the location of where it fits.

Use available information to assess the situation. If you see large amounts of debris in the air, or if local authorities say the air is badly contaminated, you may want to "shelter-in-place." Quickly bring your family and pets inside, lock doors, and close windows, air vents and fireplace dampers. Turn off air conditioning, forced air heating systems, exhaust fans and clothes dryers. Take your emergency supplies and go into the room you have designated. Seal all windows, doors and vents with plastic sheeting and duct tape or anything else you have on hand. Listen to the TV, the radio or check the Internet for instructions.

Getting Away

There may be conditions under which you will decide to get away, or there may be situations when you are ordered to leave. Plan in advance how you will assemble your family and anticipate where you will go. Choose several destinations in different directions so you have options in an emergency. If you have a car, keep at least a half tank of gas in it at all times. Become familiar with alternate routes as well as other means of transportation out of your area. If you do not have a car, plan how you will leave if you have to. Take your emergency supply kit, unless you have reason to believe it has been contaminated, and lock the door behind you. Take pets with you if you are told to evacuate, however, if you are going to a public shelter, keep in mind that they may not be allowed inside. If you believe the air may be contaminated, drive with your windows and vents closed and keep the air conditioning and heater turned off.

Working Together

Schools, daycare providers, workplaces, neighborhoods and apartment buildings, like individuals and families, should all have site-specific emergency plans. Ask about plans at the places where your family spends time: work, school and other places you frequent. If none exist, consider volunteering to help develop one. You will be better prepared to reunite your family and loved ones safely during an emergency if you think ahead, and communicate with others in advance.

Neighborhoods and Apartment Buildings

A community working together during an emergency also makes sense. Talk to your neighbors about how you can work together. Find out if anyone has specialized equipment, like a power generator, or expertise such as medical knowledge, that might help in a crisis. Decide who will check on elderly or disabled neighbors. Make backup plans for children in case you can't get home in an emergency. Sharing plans and communicating in advance is a good strategy.

Schools and Daycare

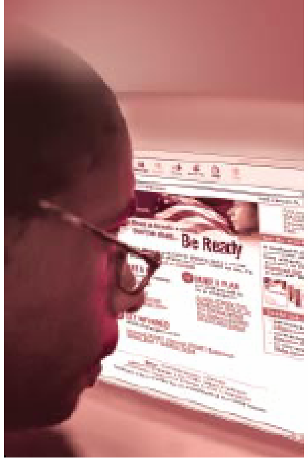
If you are a parent, or guardian of an elderly or disabled adult, make sure schools or daycare providers have emergency response plans. Ask how they will communicate with families during a crisis. Do they store adequate food, water and other emergency supplies? Find out if they are prepared to "shelter-in-place" if need be, and where they plan to go if they must get away.

Employers

If you are an employer, make sure your workplace has a building evacuation plan that is regularly practiced. Take a critical look at your heating ventilation and air-conditioning system to determine if it is secure or if it could be feasibly upgraded to better filter potential contaminants. Be sure you, and others, know how to turn off the system if necessary. Think about what to do if your employees can't go home, and make sure you have appropriate supplies on hand.

Specific Terrorist Threats

It is important to remember, there are significant differences among potential terrorist threats that will influence the decisions you make and the actions you take. By beginning a process of learning about these specific threats, you are preparing yourself to react in an emergency.



Biological Threat

A biological attack is the deliberate release of germs or other biological substances that can make you sick. Many agents must be inhaled, enter through a cut in the skin or be eaten to make you sick. Some biological agents, such as anthrax, do not cause contagious diseases. Others, like the smallpox virus, can result in diseases you can catch from people.

Unlike an explosion, a biological attack may or may not be immediately obvious. While it is possible that you will see signs of a biological attack, as was sometimes the case with the anthrax mailings, it is perhaps more likely that local health care workers will report a pattern of unusual illness or there will be a wave of sick people seeking emergency medical attention. You will probably learn of the danger through an emergency radio or TV broadcast or some other signal used in your community. Perhaps you will get a phone call or emergency response workers may come door-to-door. If you become aware of an unusual or suspicious release of an unknown substance nearby, it doesn't hurt to protect yourself. Quickly get away. Cover your mouth and nose with layers of fabric that can filter the air but still allow breathing. Examples include two to three layers of cotton such as a t-shirt, handkerchief or towel. Otherwise, several layers of tissue or paper towels may help. Wash with soap and water and contact authorities.

In the event of a biological attack, public health officials will provide information on what you should do as quickly as they can. However, it can take time for them to determine exactly what the illness is, how it should be treated and who is in danger. What you can do is watch TV, listen to the radio or check the Internet for official news including the following: Are you in the group or area authorities consider in danger? What are the signs and symptoms of the disease? Are medications or vaccines being distributed? Where? Who should get them? Where should you seek emergency medical care if you become sick?

At the time of a declared biological emergency, if a family member becomes sick, it is important to be suspicious. However, do not automatically assume you should go to a hospital emergency room or that any illness is the result of the biological attack. Symptoms of many common illnesses may overlap. Use common sense, practice good hygiene and cleanliness to avoid spreading germs, and seek medical advice.

Chemical Threat

A chemical attack is the deliberate release of a toxic gas, liquid or solid that can poison people and the environment. Watch for signs of a chemical attack such as many people suffering from watery eyes, twitching, choking, having trouble breathing or losing coordination. Many sick or dead birds, fish or small animals are also cause for suspicion. If you see signs of a chemical attack, quickly try to define the impacted area or where the chemical is coming from, if possible. Take immediate action to get away from the affected area.

If the chemical is inside a building where you are, try to get out of the building without passing through the contaminated area. Otherwise, it may be better to move as far away from where you suspect the chemical release is and "shelter-in-place." If you are outside when you see signs of a chemical attack, you must quickly decide what is the fastest way to get away from the chemical threat. Consider if you can get out of the area or if it would be better to go inside a building and follow your plan to "shelter-in-place."

If your eyes are watering, your skin is stinging, you are having trouble breathing or you simply think you may have been exposed to a chemical, immediately strip and wash. Look for a hose, fountain or any source of water. Wash with soap, if possible, but do not scrub the chemical into your skin. Seek emergency medical attention.

Nuclear Blast

A nuclear blast is an explosion with intense light and heat, a damaging pressure wave and widespread radioactive material that can contaminate the air, water and ground surfaces for miles around. While experts may predict at this time that a nuclear attack is less likely than others, terrorism by its nature is unpredictable. If there is a flash or fireball, take cover immediately, below ground if possible, though any shield or shelter will help protect you from the immediate effects of the blast and the pressure wave. In order to limit the amount of radiation you are exposed to, think about *shielding, distance* and *time*. If you have a thick shield between yourself and the radioactive materials, it will absorb more of the radiation and you will be exposed to less. Similarly, the farther away you are from the blast and the fallout, the lower your exposure. Finally, minimizing time spent exposed will also reduce your risk.

Radiation Threat or "Dirty Bomb"

A radiation threat or "Dirty Bomb" is the use of common explosives to spread radioactive materials over a targeted area. It is not a nuclear blast. The force of the explosion and radioactive contamination will be more localized. While the blast will be immediately obvious, the presence of radiation may not be clearly defined until trained personnel with specialized equipment are on the scene. As with any radiation, you want to try to limit your exposure. Think about *shielding, distance* and *time.*

In all Cases, Remain Calm.

Be prepared to adapt this information to your personal circumstances and make every effort to follow instructions received from authorities on the scene. Above all, stay calm, be patient and think before you act. With these simple preparations, you can be ready for the unexpected. If you have a working smoke detector, you understand that preparing makes sense. Get ready now.

This common sense framework is designed to launch a process of learning about citizen preparedness. For the most current information and recommendations, go to **www.ready.gov** or call **1-800-BE-READY.**

Notes

□

□

□

□

□

□

□

□

□

□

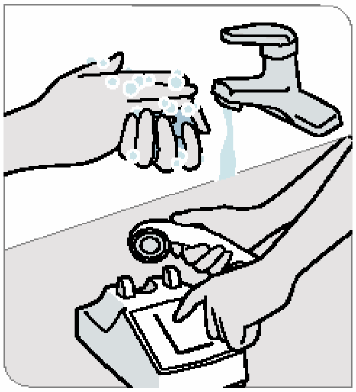
□

□

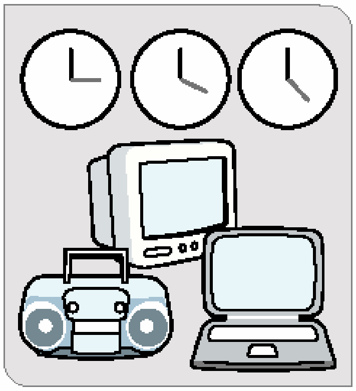
□

BE INFORMED

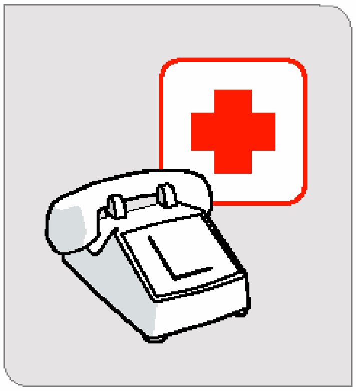
BIOLOGICAL THREAT



7. Wash with soap and water and contact authorities.



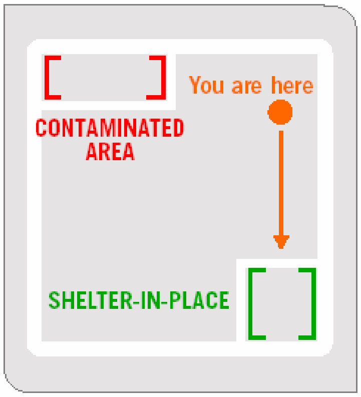
8. In the event of a biological attack, public health officials may not immediately be able to provide information on what you should do. However, you should watch TV, listen to the radio, or check the Internet for official news as it becomes available.



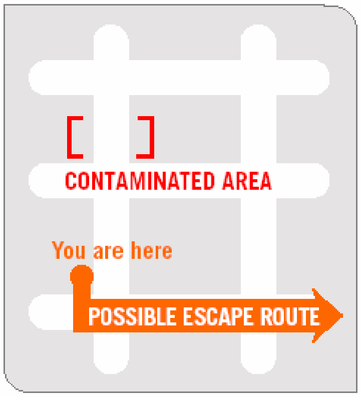
9. At the time of a declared biological emergency be suspicious, but do not automatically assume that any illness is the result of the attack. Symptoms of many common illnesses may overlap. Use common sense, practice good hygiene and cleanliness to avoid spreading germs, and seek medical advice.

BE INFORMED

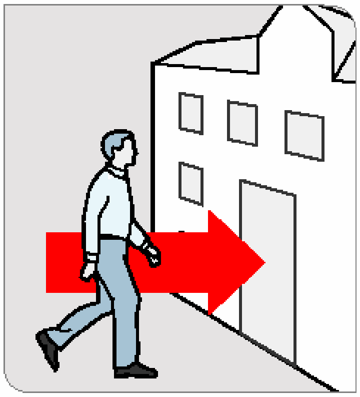
CHEMICAL THREAT



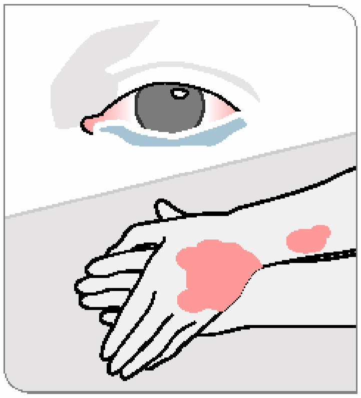
7. Otherwise, it may be better to move as far away from where you suspect the chemical release is and "shelter-in-place."



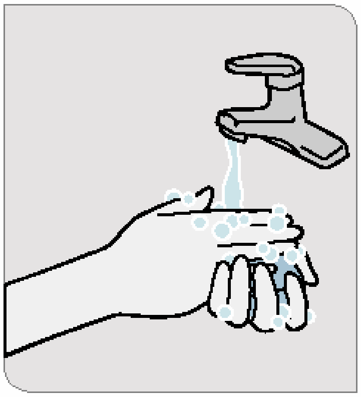
8. If you are outside when you see signs of a chemical attack, you must quickly decide the fastest way to get away from the chemical threat.



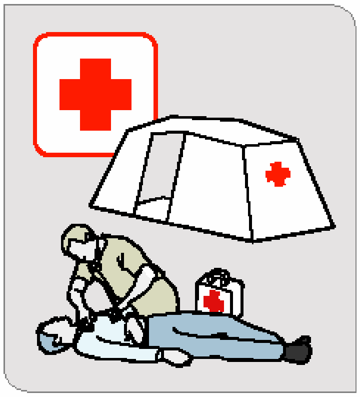
9. Consider if you can get out of the area or if it would be better to go inside a building and follow your plan to "shelter-in-place."



10. If your eyes are watering, your skin is stinging, you are having trouble breathing or you simply think you may have been exposed to a chemical, immediately strip and wash. Look for a hose, fountain, or any source of water.



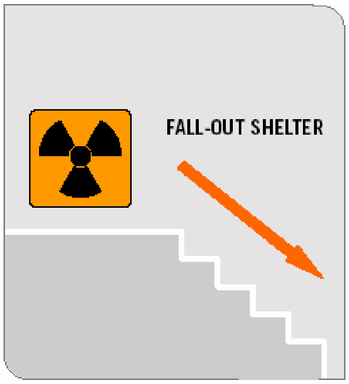
11. Wash with soap and water, if possible, but do not scrub the chemical into your skin.



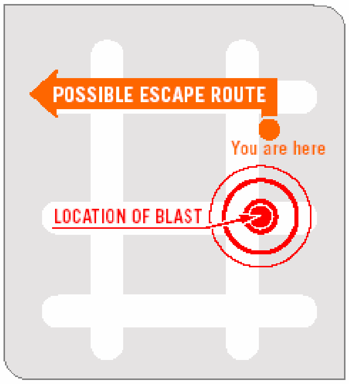
12. Seek emergency medical attention.

BE INFORMED

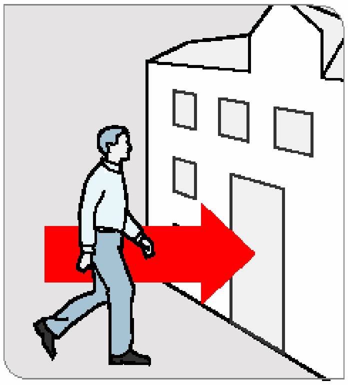
NUCLEAR BLAST



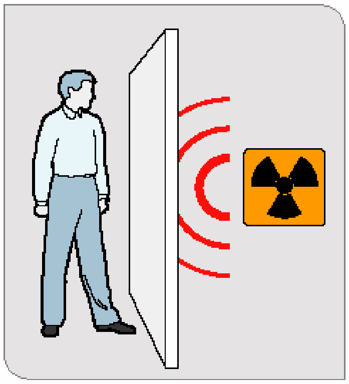
1. Take cover immediately, below ground if possible, though any shield or shelter will help protect you from the immediate effects of the blast and the pressure wave.



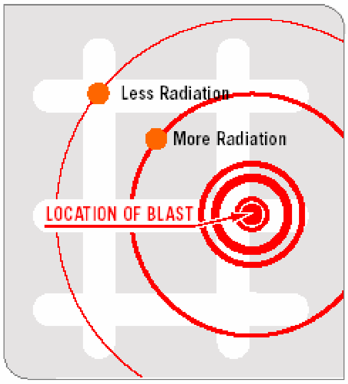
2. Consider if you can get out of the area;



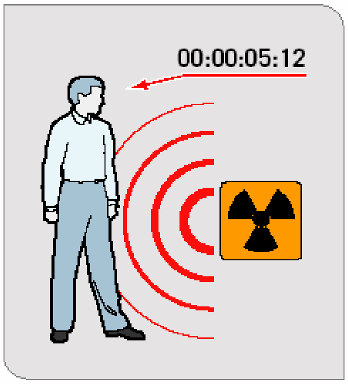
3. Or if it would be better to go inside a building and follow your plan to "shelter-in-place".



4. **Shielding**: If you have a thick shield between yourself and the radioactive materials more of the radiation will be absorbed, and you will be exposed to less.

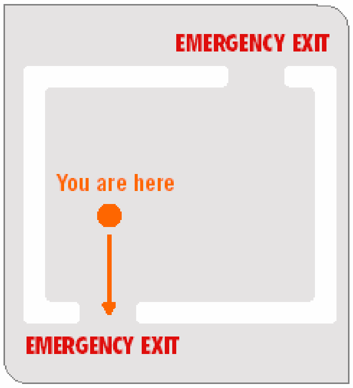


5. **Distance**: The farther away from the blast and the fallout the lower your exposure.

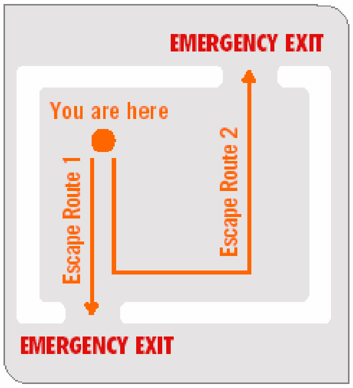


6. **Time**: Minimize time spent exposed will also reduce your risk.

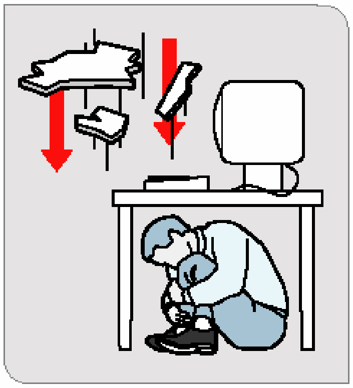
MAKE A PLAN
IN A HIGH-RISE BUILDING



1. Use available information to evaluate the situation. Note where the closest emergency exit is.



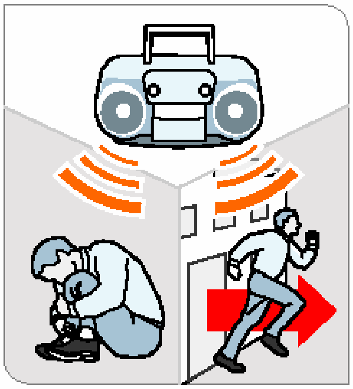
2. Be sure you know another way out of the building in case your first choice is blocked.



3. Take cover against a desk or table if things are falling.

4. Move away from file cabinets, bookshelves or other things that might fall.

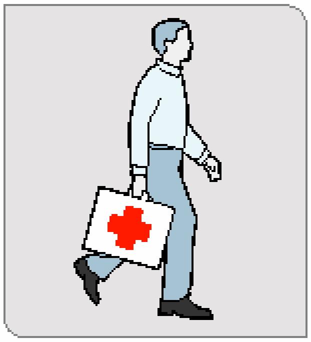
5. Face away from windows and glass. Move away from exterior walls.



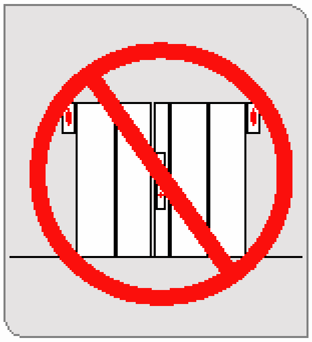
6. Determine if you should stay put, "shelter-in-place" or get away. Listen for and follow instructions from authorities.

MAKE A PLAN

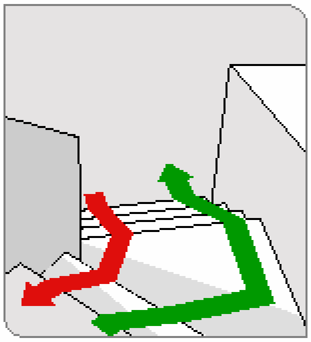
IN A HIGH-RISE BUILDING



7. Take your emergency supply kit, unless there is reason to believe it has been contaminated.



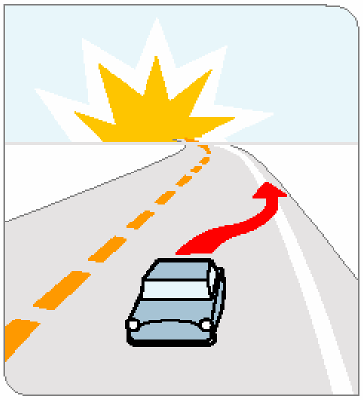
8. Do not use elevators.



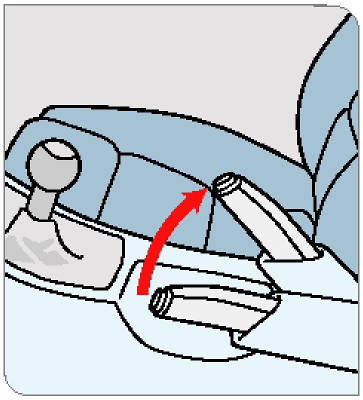
9. Stay to the right while going down stairwells to allow emergency workers to come up the stairs into the building.

MAKE A PLAN

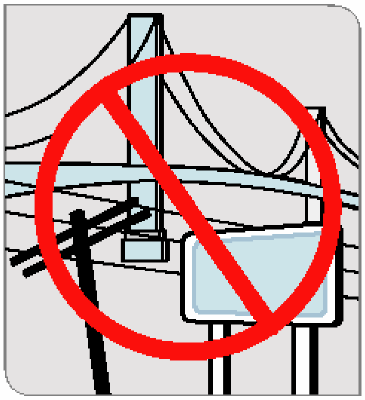
IN A MOVING VEHICLE



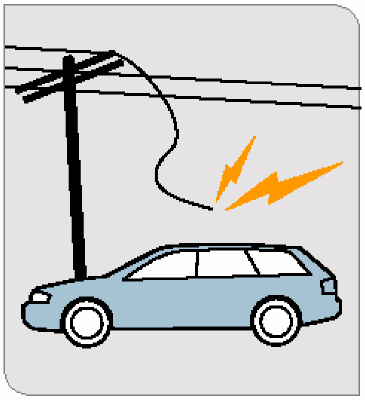
1. Use available information to evaluate the situation. If there is an explosion or other factor that makes it difficult to control the vehicle, pull over.



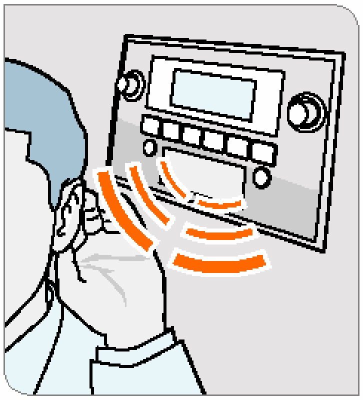
2. Stop the car, and set the parking brake.



3. If the emergency could impact the physical stability of the roadway, avoid overpasses, bridges, power lines, signs, and other hazards.



4. If a power line falls on your car you are at risk of electrical shock. Stay inside the vehicle until a trained person removes the wire.



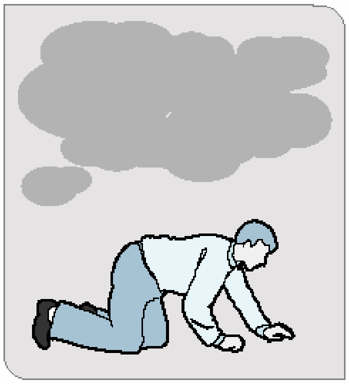
5. As with any emergency, local authorities may not immediately be able to provide information on what is happening and what you should do. However, listen to the radio for information

BE INFORMED

EXPLOSIONS

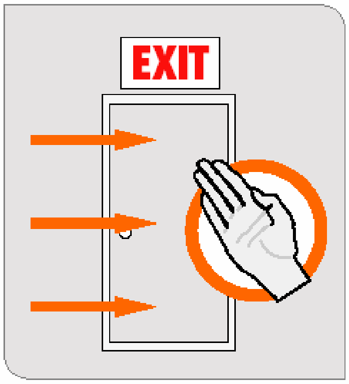
If there is fire...

1. Exit the building as quickly as possible.

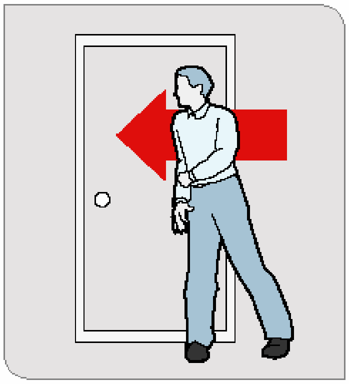


2. Crawl low in smoke.

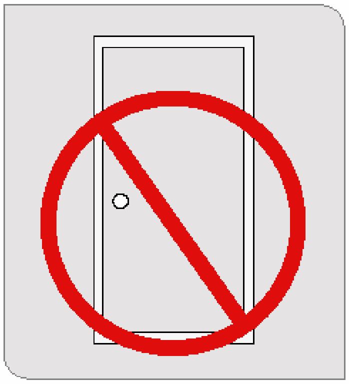
3. Use a wet cloth to cover your nose and mouth.



4. Use the back of your hand to feel the lower, middle, and upper parts of closed doors.



5. If the door is not hot, brace yourself against the door and open it slowly.



6. Do not open the door if it is hot. Look for another way out.

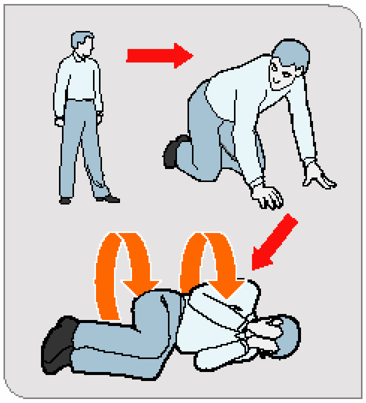
BE INFORMED

EXPLOSIONS If there is fire...

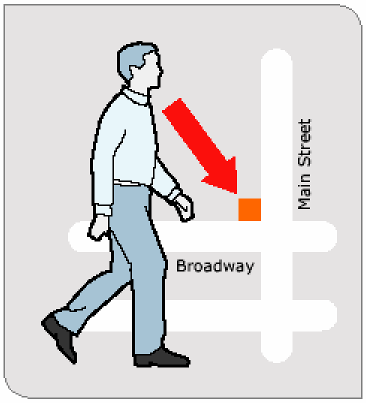
You are here
ELEVATOR
FIRE EXIT

7. Use appropriate fire exits, not elevators.

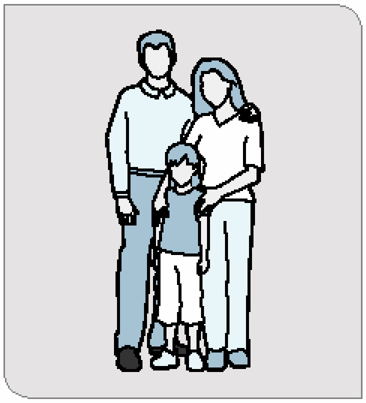
8. If you catch fire, do not run!



9. Stop, Drop and Roll.

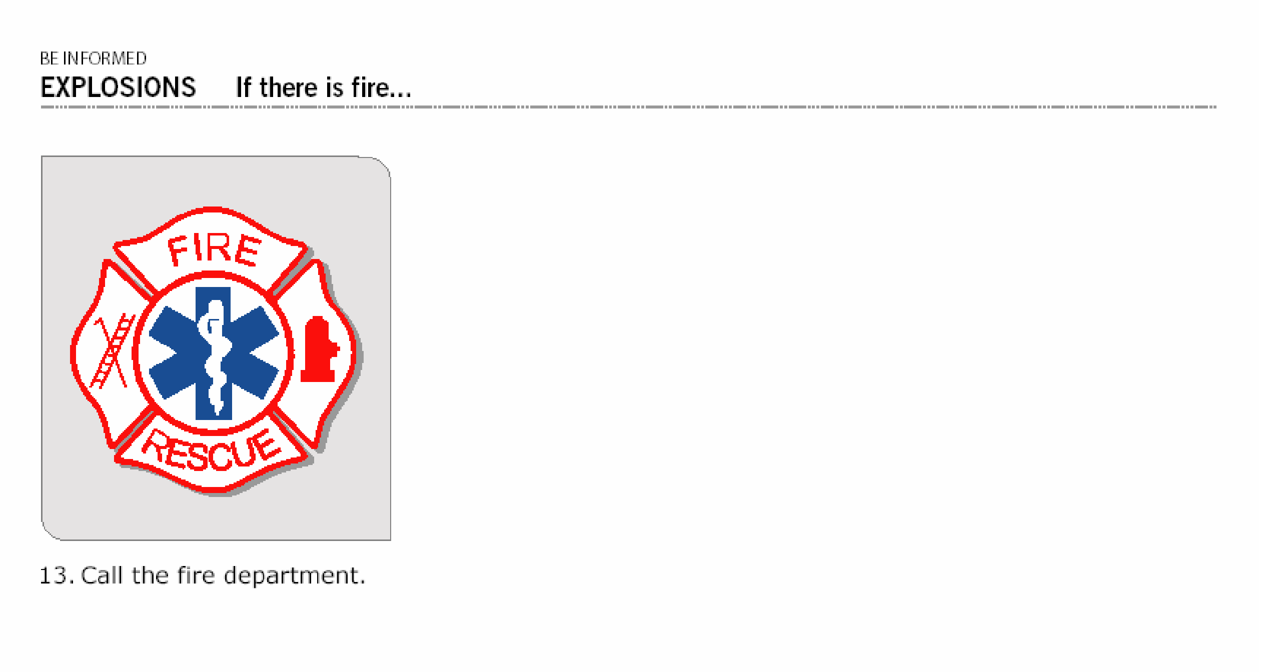


10. If you are at home, go to previously designated meeting place.



11. Account for your family members.

12. Do not go back into a burning building and carefully supervise small children.



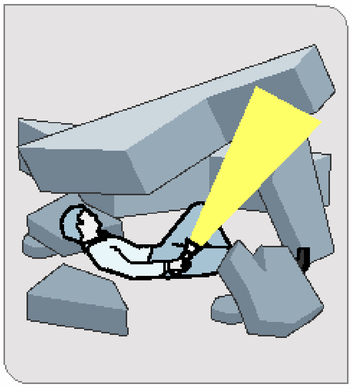
BE INFORMED

EXPLOSIONS **If there is fire...**

13. Call the fire department.

BE INFORMED

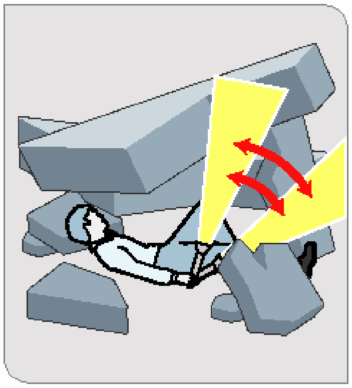
EXPLOSIONS If you are trapped in debris...



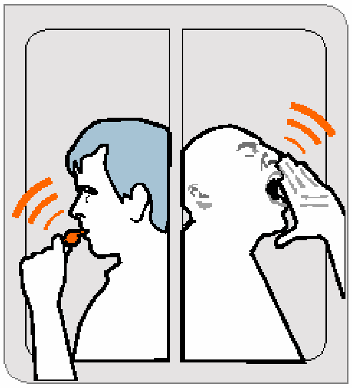
1. If possible, use a flashlight to signal your location.

2. Avoid unnecessary movement so that you don't kick up dust.

3. Cover your mouth and nose with anything you have on hand. Dense weave cotton material can create a good filter. Try to breathe through the material.



4. Tap on a pipe or wall so that rescuers can hear where you are.



5. Use a whistle if one is available. Shout only as a last resort - shouting can cause a person to inhale dangerous amounts of dust.

TORNADO • FLASH FLOOD • EARTHQUAKE • WINTER STORM • HURRICANE • FIRE • HAZARDOUS MATERIALS SPILL

Food and Water in an Emergency

How to Store Water

Store your water in thoroughly washed plastic, glass, fiberglass or enamel-lined metal containers. Never use a container that has held toxic substances. Plastic containers, such as soft drink bottles, are best. You can also purchase food-grade plastic buckets or drums.

Seal water containers tightly, label them and store in a cool, dark place. Rotate water every six months.

Emergency Outdoor Water Sources

If you need to find water outside your home, you can use these sources. Be sure to purify the water according to the instructions on page 3 before drinking it.

- Rainwater
- Streams, rivers and other moving bodies of water
- Ponds and lakes
- Natural springs

Avoid water with floating material, an odor or dark color. Use saltwater only if you distill it first. You should not drink flood water.

If an earthquake, hurricane, winter storm or other disaster strikes your community, you might not have access to food, water and electricity for days, or even weeks. By taking some time now to store emergency food and water supplies, you can provide for your entire family. This brochure was developed by the Federal Emergency Management Agency in cooperation with the American Red Cross and the U.S. Department of Agriculture.

Having an ample supply of clean water is a top priority in an emergency. A normally active person needs to drink at least two quarts of water each day. Hot environments can double that amount. Children, nursing mothers and ill people will need even more. You will also need water for food preparation and hygiene. Store a total of at least one gallon per person, per day. You should store at least a two-week supply of water for each member of your family.

If supplies run low, never ration water. Drink the amount you need today, and try to find more for tomorrow. You can minimize the amount of water your body needs by reducing activity and staying cool.

Federal Emergency Management Agency

American Red Cross

FOOD SUPPLIES

Short-Term Food Supplies

Even though it is unlikely that an emergency would cut off your food supply for two weeks, you should prepare a supply that will last that long.

The easiest way to develop a two-week stockpile is to increase the amount of basic foods you normally keep on your shelves.

Storage Tips

- Keep food in a dry, cool spot—a dark area if possible.
- Keep food covered at all times.
- Open food boxes or cans carefully so that you can close them tightly after each use.
- Wrap cookies and crackers in plastic bags, and keep them in tight containers.
- Empty opened packages of sugar, dried fruits and nuts into screw-top jars or air-tight cans to protect them from pests.
- Inspect all food for signs of spoilage before use.
- Use foods before they go bad, and replace them with fresh supplies, dated with ink or marker. Place new items at the back of the storage area and older ones in front.

Nutrition Tips

During and right after a disaster, it will be vital that you maintain your strength. So remember:

- Eat at least one well-balanced meal each day.
- Drink enough liquid to enable your body to function properly (two quarts a day).
- Take in enough calories to enable you to do any necessary work.
- Include vitamin, mineral and protein supplements in your stockpile to assure adequate nutrition.

Hidden Water Sources in Your Home

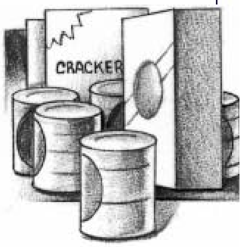
If a disaster catches you without a stored supply of clean water, you can use the water in your hot-water tank, pipes and ice cubes. As a last resort, you can use water in the reservoir tank of your toilet (not the bowl).

Do you know the location of your incoming water valve? You'll need to shut it off to stop contaminated water from entering your home if you hear reports of broken water or sewage lines.

To use the water in your pipes, let air into the plumbing by turning on the faucet in your house at the highest level. A small amount of water will trickle out. Then obtain water from the lowest faucet in the house.

To use the water in your hot-water tank, be sure the electricity or gas is off, and open the drain at the bottom of the tank. Start the water flowing by turning off the water intake valve and turning on a hot-water faucet. Do not turn on the gas or electricity when the tank is empty.

When Food Supplies Are Low



If activity is reduced, healthy people can survive on half their usual food intake for an extended period and without any food for many days. Food, unlike water, may be rationed safely, except for children and pregnant women.

If your water supply is limited, try to avoid foods that are high in fat and protein, and don't stock salty foods, since they will make you thirsty. Try to eat salt-free crackers, whole grain cereals and canned foods with high liquid content.

You don't need to go out and buy unfamiliar foods to prepare an emergency food supply. You can use the canned foods, dry mixes and other staples on your cupboard shelves. In fact, familiar foods are important. They can lift morale and give a feeling of security in time of stress. Also, canned foods won't require cooking, water or special preparation. Following are recommended short-term food storage plans.

Special Considerations

As you stock food, take into account your family's unique needs and tastes. Try to include foods that they will enjoy and that are also high in calories and nutrition. Foods that require no refrigeration, preparation or cooking are best.

Individuals with special diets and allergies will need particular attention, as will babies, toddlers and elderly people. Nursing mothers may need liquid formula, in case they are unable to nurse. Canned dietetic foods, juices and soups may be helpful for ill or elderly people.

Make sure you have a manual can opener and disposable utensils. And don't forget nonperishable foods for your pets.

How to Cook If the Power Goes Out

For emergency cooking you can use a fireplace, or a charcoal grill or camp stove can be used outdoors. You can also heat food with candle warmers, chafing dishes and fondue pots. Canned food can be eaten right out of the can. If you heat it in the can, be sure to open the can and remove the label first.

Three Ways to Purify Water

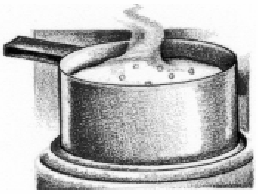
In addition to having a bad odor and taste, contaminated water can contain microorganisms that cause diseases such as dysentery, typhoid and hepatitis. You should purify all water of uncertain purity before using it for drinking, food preparation or hygiene.

There are many ways to purify water. None is perfect. Often the best solution is a combination of methods.

Two easy purification methods are outlined below. These measures will kill most microbes but will not remove other contaminants such as heavy metals, salts and most other chemicals. Before purifying, let any suspended particles settle to the bottom, or strain them through layers of paper towel or clean cloth.

BOILING. Boiling is the safest method of purifying water. Bring water to a rolling boil for 3-5 minutes, keeping in mind that some water will evaporate. Let the water cool before drinking.

Boiled water will taste better if you put oxygen back into it by pouring the water back and forth between two clean containers. This will also improve the taste of stored water.



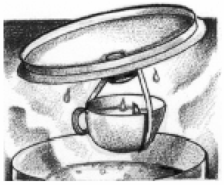
DISINFECTION. You can use household liquid bleach to kill microorganisms. Use only regular household liquid bleach that contains 5.25 percent sodium hypochlorite. Do not use scented bleaches, colorsafe bleaches or bleaches with added cleaners.

Add 16 drops of bleach per gallon of water, stir and let stand for 30 minutes. If the water does not have a slight bleach odor, repeat the dosage and let stand another 15 minutes.

The only agent used to purify water should be household liquid bleach. Other chemicals, such as iodine or water treatment products sold in camping or surplus stores that do not contain 5.25 percent sodium hypochlorite as the only active ingredient, are not recommended and should not be used.

While the two methods described above will kill most microbes in water, distillation will remove microbes that resist these methods, and heavy metals, salts and most other chemicals.

DISTILLATION. Distillation involves boiling water and then collecting the vapor that condenses back to water. The condensed vapor will not include salt and other impurities. To distill, fill a pot halfway with water. Tie a cup to the handle on the pot's lid so that the cup will hang right-side-up when the lid is upside-down (make sure the cup is not dangling into the water) and boil the water for 20 minutes. The water that drips from the lid into the cup is distilled.



FOOD STORAGE

Shelf-life of Foods for Storage

Here are some general guidelines for rotating common emergency foods.

- Use within six months:
  - Powdered milk *(boxed)*
  - Dried fruit *(in metal container)*
  - Dry, crisp crackers *(in metal container)*
  - Potatoes
- Use within one year:
  - Canned condensed meat and vegetable soups
  - Canned fruits, fruit juices and vegetables
  - Ready-to-eat cereals and uncooked instant cereals *(in metal containers)*
  - Peanut butter
  - Jelly
  - Hard candy and canned nuts
  - Vitamin C
- May be stored indefinitely *(in proper containers and conditions):*
  - Wheat
  - Vegetable oils
  - Dried corn
  - Baking powder
  - Soybeans
  - Instant coffe, tea and cocoa
  - Salt
  - Noncarbonated soft drinks
  - White rice
  - Bouillon products
  - Dry pasta
  - Powdered milk *(in nitrogen-packed cans)*

DISASTER SUPPLIES

Supplies

It's 2:00 a.m. and a flash flood forces you to evacuate your home—fast. There's no time to gather food from the kitchen, fill bottles with water, grab a first-aid kit from the closet and snatch a flashlight and a portable radio from the bedroom. You need to have these items packed and ready in one place before disaster strikes.

Pack at least a three-day supply of food and water, and store it in a handy place. Choose foods that are easy to carry, nutritious and ready-to-eat. In addition, pack these emergency items:

- Medical supplies and first aid manual
- Hygiene supplies
- Portable radio, flashlights and extra batteries
- Shovel and other useful tools
- Household liquid bleach to purify drinking water.
- Money and matches in a waterproof container
- Fire extinguisher
- Blanket and extra clothing
- Infant and small children's needs *(if appropriate)*
- Manual can opener

If the Electricity Goes Off. . .

FIRST, use perishable food and foods from the refrigerator.

THEN, use the foods from the freezer. To minimize the number of times you open the freezer door, post a list of freezer contents on it. In a well-filled, well-insulated freezer, foods will usually still have ice crystals in their centers (meaning foods are safe to eat) for at least three days.

FINALLY, begin to use non-perishable foods and staples.

Learn More

If you are interested in learning more about how to prepare for emergencies, contact your local or State Office of Emergency Management or local American Red Cross chapter, or write to

FEMA
PO BOX 2012
JESSUP MD 20794-2012

and ask for any of the following publications:

Emergency Preparedness Checklist
(L-154) Item #8-0872
ARC 4471

Your Family Disaster Supplies Kit
(L-189) Item #8-0941
ARC 4463

Your Family Disaster Plan
(L-191) Item #8-0954
ARC 4466

Are You Ready? Your Guide to Disaster Preparedness
(H-34) Item #8-0908

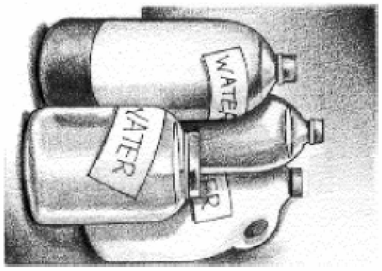
Emergency Preparedness Publications
(L-164) Item #8-0822

Your Local Contact is:

ARC-5055
FEMA©-L210
November 1994

TORNADO • FLASH FLOOD • EARTHQUAKE • WINTER STORM

Food & Water in an Emergency



In a disaster, you might be cut off from food, water and electricity for days. By preparing emergency provisions, you can turn what could be a life-threatening situation into a manageable problem.

Federal Emergency Management Agency

American Red Cross

HURRICANE • FIRE • HAZARDOUS MATERIALS SPILL

APPENDIX E

INDEX

Subject **Paragraph**