

DRAFT

CONTENTS

ACRONYMS.....	vii
1.0 PURPOSE.....	1
2.0 SCOPE.....	2
3.0 GENERAL INFORMATION RELATING TO OPERATIONAL SECURITY.....	3
3.1 DAILY ROUTINE OPERATIONS.....	3
3.2 OFF-NORMAL AND EMERGENCY OPERATIONS.....	4
3.3 ASSUMPTIONS.....	4
3.3.1 Responsibilities of Staff Members.....	5
3.3.2 Emergency Preparedness.....	5
3.3.3 Emergency Situations.....	5
3.3.4 Staff Supervisors.....	6
3.3.5 Safety and Communications.....	6
3.3.6 Emergency Command and Communication Post Minimum Equipment....	7
3.3.7 Staff Training.....	7
3.4 OPERATIONAL PROCEDURES GUIDE.....	8
4.0 PHYSICAL SECURITY AND PERSONAL SAFETY.....	10
4.1 ANTI-TERRORISM OFFICER.....	10
4.2 ACCESS CONTROL REQUIREMENTS.....	11
4.2.1 Access Control Under General Conditions.....	11
4.2.2 Access Control Under Force Protection Conditions.....	12
4.3 MAIL HANDLING PROCEDURES.....	12
4.3.1 Initial Mail Screening.....	13
4.3.2 Suspicious Mail/Packages.....	13
4.4 RECRUITERS AND OPERATIONAL INFORMATION CONTROL.....	14
4.4.1 General Information Control.....	14
4.4.2 Computers.....	14
4.4.3 Unclassified Information.....	15
4.4.4 Classified Information.....	16
4.5 CRIME PREVENTION TACTICS.....	16

4.5.1	Develop an Awareness of the Environment.....	17
4.5.2	Educate Yourself About Risks.....	17
4.5.3	Keys Components to Security.....	18
4.5.4	Locks and Keys.....	19
4.5.5	Crime Prevention Checklist.....	20
4.6	SURVEILLANCE DETECTION PRACTICES.....	20
4.6.1	Introduction.....	20
4.6.2	Simple Counter-Surveillance Techniques.....	21
4.6.3	How Terrorists/Criminals Select a Target or a Victim.....	22
4.6.4	Potential Targets.....	23
4.6.5	What the Terrorist/Criminal Needs to Know.....	24
4.6.6	Where to Look.....	25
4.6.7	What to Look For.....	27
4.6.8	How and What to Report.....	30
4.6.9	Area Security Coordinator.....	33
4.6.10	When to Intervene.....	34
4.6.11	Potential Actions to Further Improve Security.....	34
4.6.12	Sample Report.....	34
4.6.13	A Few Key Reminders.....	35
4.6.14	Protecting Yourself Against Stalkers/Stalking.....	35
4.7	PROCEDURES FOR SPECIAL ACTIVITIES.....	36
4.7.1	Planning and Preparation Procedures.....	37
4.7.2	General Security.....	37
4.7.3	Vehicle Security.....	38
4.8	REPORTING REQUIREMENTS.....	38
4.8.1	Medical Emergency.....	39
4.8.2	Suspicious Activity.....	39
4.8.3	Contact Numbers.....	39
4.8.4	Utility Failures.....	40
4.9	VEHICLE SECURITY PROCEDURES.....	41
4.9.1	Vehicle Security Precautions.....	41

4.9.2	Vehicle Security at ATMs	43
4.9.3	Protecting Yourself Against Sexual Assault.....	43
4.10	PHYSICAL SECURITY EQUIPMENT	44
5.0	EMERGENCY MEDICAL PLANS AND CBRNE PLANS	45
5.1	MEDICAL PLANS AND CONTACT INFORMATION	45
5.1.1	Emergency Telephone Numbers.....	45
5.1.2	Emergency Actions.....	46
5.2	CHEMICAL, BIOLOGICAL, RADIATION, NUCLEAR, AND EXPLOSIVE (CBRNE) PLANS AND INFORMATION	46
5.2.1	Hazards From CBRNE Attacks	46
5.3	PREVENTION AND ACTIONS BEFORE ANY EVENT	51
5.3.1	Actions if Attack is Expected	51
5.3.2	Actions During an Event.....	52
5.3.3	Actions After the Event	52
6.0	LOCAL EMERGENCY SERVICES GUIDANCE	54
6.1	BOMB THREAT PROCEDURES	54
6.2	FIRE PROTECTION PROGRAM	55
6.3	CIVIL DISTURBANCES AND PROTESTS	56
6.4	DISASTER AND EMERGENCY PLANS	58
6.4.1	Severe Weather/Tornado	58
6.4.2	Floods.....	60
6.4.3	Lightning.....	60
6.4.4	Utility Failure.....	61
6.4.5	Chemical Spills	61
6.4.6	Menacing Person/Weapons Threat	62
6.4.7	Harassing/Obscene Telephone Calls.....	62
6.4.8	Kidnapping/Hostage Situation	63
ATTACHMENT A	POINT OF CONTACT LIST – RECRUITING COMMAND OPERATIONAL SECURITY MANUAL	A-1
ATTACHMENT B 1	PHYSICAL SECURITY FEATURES – GENERAL RESPONSIBILITIES / PROCEDURES	B 1-1

ATTACHMENT B 2	CHECKLIST FOR INITIAL SCREENING OF SUSPICIOUS MAIL/PACKAGES	B 2-1
ATTACHMENT B 3	CHECKLIST FOR CRIME PREVENTION TACTICS	B 3-1
ATTACHMENT B 4	VEHICLE SEARCH CHECKLIST	B 4-1
ATTACHMENT B 5	BOMB THREAT CHECKLIST	B 5-1
ATTACHMENT B 6	EMERGENCY ACTIONS CHECKLIST FOR FIRE PROTECTION	B 6-1
ATTACHMENT B 7	EMERGENCY ACTIONS FOR CHEMICAL SPILLS.....	B 7-1
ATTACHMENT B 8	KIDNAPPING / HOSTAGE SITUATION CHECKLIST	B 8-1
ATTACHMENT B 9	UNUSUAL OBSERVATION REPORT	B 9-1
ATTACHMENT C	OPERATING INSTRUCTIONS/MANUALS	C-1
ATTACHMENT D	REFERENCES	D-1

ACRONYMS

AT/FP	Anti-Terrorism/Force Protection
ATM	Automatic Teller Machine
ATO	Anti-Terrorism Officer
CBRNE	Chemical, Biological, Radiation, Nuclear, and Explosive
CDC	Center for Disease Control
CONUS	Continental United States
CPR	Cardiopulmonary Resuscitation
DoD	Department of Defense
FBI	Federal Bureau of Investigation
GSA	Government Services Administration
IED	Improvised Explosive Device
IND	Improvised Nuclear Device
LPO	Leading Petty Officer
MSDS	Material Safety Data Sheet
NCOIC	Non-Commissioned Officer-in-Charge
OCONUS	Outside Continental United States
OIC	Officer-in-Charge
OSM	Operational Security Manual
POV	Privately Owned Vehicle
RDD	Radiological Dispersal Device

OPERATIONAL SECURITY MANUAL

1.0 PURPOSE

This Operational Security Manual (OSM) contains general security and crime prevention procedures and tactics as well as emergency response and recovery actions that may be needed in the event of a criminal or terrorist attack on a recruiting office, to include environmental response to chemical, biological, and radiological events. The manual applies generically to Continental United States (CONUS) recruiting offices and Outside Continental United States (OCONUS) stations located in Alaska, Hawaii, Guam, Puerto Rico, and the Virgin Islands. In addition to the Purpose, Scope and the General Information Related to Operational Security sections, this manual is divided into three other sections designed to explain the definition, concept, reasoning, and protective measures or procedures to be used by recruiting personnel. These three sections of the OSM are identified as:

4.0 Physical Security and Personal Safety

5.0 Medical Plans and Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Plans

6.0 Local Emergency Services Guidance

The basic procedures outlined in this manual are to enhance the overall daily operation of the facility as well as to protect persons and property during emergency situations through effective use of available resources. Whenever an emergency affecting the recruiting station reaches proportions that cannot be handled by routine measures, the person in charge, or his/her designate, may declare an emergency situation and these contingency guidelines described may be implemented. There are two implementations of this guide. Since an emergency may be sudden and without warning, these procedures are designed to be flexible in order to accommodate contingencies of various magnitudes. This may range from simple guidelines for receiving daily mail to extreme situations, such as criminal acts or severe weather conditions.

2.0 SCOPE

These procedures apply to all recruiting facility personnel, buildings, property and vehicles leased and/or owned and maintained by the various Department of Defense (DoD) Recruiting Commands.

3.0 GENERAL INFORMATION RELATING TO OPERATIONAL SECURITY

This section identifies general information that relates to topic areas that are addressed in detail in the following sections of this manual. It must be understood by all personnel that any of the topic areas identified may occur at any time during normal daily operations, as well as at any other times (nights, holidays, weekends). It is essential that all personnel are thoroughly familiar with the content and procedures discussed in the **Operational Security Manual** for the well being of all workers, applicants, and other visitors; and to maintain the security of facilities, equipment and adjacent grounds. The procedures discussed are provided as guidelines to assist in determining the appropriate response and/or procedure. This list of topic areas covered in this manual is not inclusive of all situations and, therefore, must be used as a guide to good common sense. Any additions and/or deletions should be addressed according to the uniqueness of each recruiting facility.

3.1 DAILY ROUTINE OPERATIONS

Routine operations are defined as daily tasks in support of the recruiting effort. This includes opening and closing the office, receipt of mail and packages, reporting to the Command, public presentations both on and off site, driving DoD vehicles, association with public entities, and ensuring the well being of all staff personnel and visitors. Because an individual's daily tasks often become a "Daily Routine", we sometimes begin to take everything for granted and occasionally forget that all aspects of the job have their own vulnerabilities associated with each and every task. For the most part, our daily routine seems to be harmless and we neglect to see appropriate warnings. Information and procedures that are important to the "daily routine", such as mail procedures, vehicle security, CBRNE, bomb threats, crime prevention tactics, disaster and emergency planning, reporting requirements and so forth are discussed in detail in Sections 4.0 to 6.0 of this manual.

3.2 OFF-NORMAL AND EMERGENCY OPERATIONS

The following definitions of an emergency are provided as guidelines to assist in determining the appropriate response.

- **Off-Normal Operations**: any incident, potential or actual, which will not seriously affect the overall functional capacity of the recruiting station. Generally handled through routine procedures not requiring major policy considerations or decisions.
- **Major Emergency**: any incident, potential or actual, which affects personnel and/or the entire building or buildings, and which will disrupt the overall operations of the recruiting station. Outside emergency services will probably be required, as well as major efforts from other support services. Major decisions and/or policy considerations will usually be required from the local Command during times of a major emergency.
- **Disaster**: any event or occurrence that has taken place and has seriously impaired or halted the operations of the recruiting station. In some cases, mass casualties and severe property damage may be sustained. A coordinated effort of all available resources is required to effectively control the situation. Outside emergency services will be essential. In all cases of disaster, all personnel present shall assemble at a pre-designated emergency assembly point, establish a *temporary* Emergency Command and Communication Post, and commence execution of the appropriate support and operational plans.

3.3 ASSUMPTIONS

This **Operational Security Manual** is predicated on a realistic approach to the problems likely to be encountered during the routine workday, a major emergency, or a disaster. The following information will generally apply.

3.3.1 Responsibilities of Staff Members

The Commander, Officer-in-Charge (OIC), or the Non-Commissioned Officer-in-Charge/Leading Petty Officer (NCOIC/LPO), as appropriate, has the following general responsibilities prior to and during any emergency. However, he/she may appoint a specific person as Building/Facility Coordinator for each recruiting facility.

When Services are co-located within the same facility/building, every effort must be made to coordinate response actions and responsibilities among the Services. While each Service will be required to make the necessary notifications within their own Command and take the required actions within their own offices within the facility, there needs to be coordination between the Services regarding notification of other agencies, response teams and organizations outside the Military Recruiting Command. Consideration should be given to the establishment of a written agreement between the Services that are co-located within the same facility that outlines the agreed upon emergency assembly area, who will have responsibility to establish and man the temporary Emergency Command Post, and who will have responsibility to notify other agencies, response teams and organizations outside of their respective individual Commands.

3.3.2 Emergency Preparedness

Building evacuation information shall be distributed to all recruiting facility personnel with follow-up discussions and on-the-job training and/or explanation, as required.

Time shall be allowed for training all personnel in emergency procedures, notifications and techniques, such as fire extinguisher usage, first aid, Cardiopulmonary Resuscitation (CPR) and building evacuation procedures. With Command approval, outside sources may be called for training assistance, such as the local fire department, local law enforcement criminal investigation unit, and the local chapter of the American Red Cross.

3.3.3 Emergency Situations

If an emergency situation develops, the recruiting staff should:

- Inform facility personnel of the emergency situation.

- Initiate required emergency procedures, as applicable, such as evacuation of the building(s).
- Evaluate the impact that the emergency has on the activities of personnel and take appropriate action.
- Maintain communications with your Command, local officials, emergency responders and other agencies that may provide assistance, as may be required/necessary.

3.3.4 Staff Supervisors

Each recruiting supervisor and/or his/her designee has the responsibility to:

- Educate his/her recruiters and/or other employees concerning the emergency procedures, as well as evacuation procedures, for their building and/or recruiting facility.
- Survey and evaluate his/her building or assigned area for hazards and report any identified hazards. Prepare personnel to take corrective action to minimize hazards to personnel, facilities and/or equipment (e.g., move personnel away from windows, electrical or other hazards, etc.)
- Inform staff of an emergency and initiate emergency procedures as outlined in this guide and other applicable local safety manuals/procedures.

3.3.5 Safety and Communications

When an emergency either occurs or is imminent, it shall be the responsibility of the senior recruiter present to establish an appropriate line of communications. As much as possible, the Command structure emergency personnel are to be kept fully aware of the situation. However, the safety of personnel comes first and foremost. As much as practical, a *temporary* Emergency Command and Communication Post should be established to maintain communication with Command and outside emergency response personnel. The temporary Emergency Command and Communication Post should be manned and remain operational until relieved or replaced by local authorities or Command personnel.

3.3.6 Emergency Command and Communication Post Minimum Equipment

The following equipment is suggested minimum equipment for the emergency command and communication post.

- Portable hand-held radios
- Portable cellular telephone
- Portable public address system (bull horn)
- First aid kit
- Emergency Telephone Directory
- Local telephone directory and yellow pages
- Emergency Operations Directives/manuals
- Operational Security Manual

3.3.7 Staff Training

The appropriate level of training for the staff is important to maintain a consistent level of security awareness for all personnel. All training shall be documented in each individual's personnel record.

- Initial Recruiter Training:
 - Upon assignment, new personnel will receive training in operational security of personnel, facilities and vehicles.
 - The initial training should occur within 30 calendar days of assignment and will encompass all procedures identified in Sections 4.0, 5.0, and 6.0 of this manual, at a minimum.

- Refresher Training:
 - Assigned personnel will undergo refresher training annually. The refresher training should consist of formal discussions of the security procedures identified in Sections 4.0, 5.0, and 6.0 of this manual. Refresher training may also serve as an annual review of the Operational Security Manual for the purpose of ensuring that all pertinent local information (names, addresses/locations, phone numbers, etc.) is current. All necessary changes shall be incorporated into the OSM at this time.

3.4 OPERATIONAL PROCEDURES GUIDE

Operational procedures have been developed to serve as guides to assist recruiting facility personnel in dealing with both routine and emergency situations. It is the responsibility of the Recruiting Supervisor in each facility to ensure that all persons assigned are familiar with the contents and location of this manual and their responsibilities related to Operational Security. These procedures are provided in Sections 4.0, 5.0, and 6.0 of this manual. Section 4.0 discusses “Physical Security and Personal Safety” issues; Section 5.0 discusses “Medical Plans and CBRNE Plans”; and Section 6.0 provides “Local Emergency Services Guidance.”

A Point of Contact list is provided in Attachment A and each recruiting facility is required to fill in the necessary information for their location. It is also required that this list be maintained in a current status at all times. As contact personnel, phone numbers, and/or addresses change, this list must also be changed. An out-of-date contact list will only serve to compound the problem in a case of emergency or disaster. Maintain the master copy of the contact list in its present form. It is suggested that copies of the contact list be made, filled out as appropriate, placed in the appropriate section of the OSM, and distributed to facility personnel for quick reference in case of incident or emergency.

Related forms and checklists are located on Attachment B. These forms and checklists are also required to be filled out for each recruiting facility and must be maintained in a current and up-to-date fashion at all times. Maintain the master copy of the forms and checklists in their present form. It is suggested that copies of the forms and checklists be made, filled out as appropriate,

placed in the appropriate section of the OSM, and distributed to facility personnel for quick reference in case of incident or emergency.

Manufacturer's Operating Instructions/Manuals for pertinent physical security features are located in Attachment C.

4.0 PHYSICAL SECURITY AND PERSONAL SAFETY

This section describes the procedures and guidelines to be followed in the areas of physical security of facilities and vehicles and safety for all personnel. Information is also provided regarding point of contact information and reporting requirements pertaining to physical security and personnel safety.

This section of the OSM is divided into ten (10) discrete subsections to enable users to rapidly locate pertinent information and requirements in case of emergency. A point-of-contact list is located at Attachment A. Local information (e.g., Command Anti-Terrorism Officer, Police and Fire Departments, etc.) will need to be filled in for each recruiting facility. Checklists and forms to be filled out locally are located in Attachment B.

All Recruiting Command personnel are required to be totally familiar with the contents of this section of the OSM and supervisory personnel are responsible to insure that all contact information and required forms are maintained current at all times.

4.1 ANTI-TERRORISM OFFICER

An Anti-Terrorism Officer (ATO) is designated for each local recruiting Command. The ATO is normally the principle point of contact for all matters relating to real or potential terrorism incidents, and anti-terrorism planning and training issues. The ATO should be notified immediately by the affected recruiting facility in the event of any real or perceived terrorism related incident.

The name, address and contact numbers for the Command ATO are located in contact list provided at Attachment A. It is the responsibility of the recruiting facility supervisor to ensure that the ATO contact information in Attachment A is maintained current at all times.

4.2 ACCESS CONTROL REQUIREMENTS

This section discusses Access Control Requirements under normal or general conditions and under each Force Protection Condition. Access Control is the responsibility of all personnel.

4.2.1 Access Control Under General Conditions

Keys and Access Codes

The authorization and issue of keys or access codes will be granted to those people recommended by their recruiting supervisor. Records of each individual having access and their level of access to specific buildings, areas, safes and government owned vehicles will be maintained by Recruiting OIC, NCOIC or Supervisor, as appropriate.

All issued keys are the property of the government and, as such, they are subject to recall at any time. Keys must be picked up and signed for by the individual for whom they were ordered. *The person who signs for the key(s) and/or access code(s) is responsible for their custody and control at all times.*

When keys are no longer needed or a person is transferred, all keys must be returned to proper authority. When changing departments or offices, the old key(s) must be turned in at the time new keys are issued. If an employee fails to return his/her keys to the proper authority, every effort will be made to recover the keys. If recovery is not effective, the locks must be changed or re-keyed within a reasonable period of time, preferably within one week. In the case of access codes, all codes will be changed upon personnel transfers, terminations or changes in the level of access. Lost/stolen keys must be reported to the recruiting supervisor immediately.

Physical Security Hardware

Each facility will have physical security hardware based upon the facility type, location, construction, and lease agreements. Attachment B 1 identifies general responsibilities and procedures for the different types of physical security hardware. Each facility recruiting supervisor should refer to Attachment B 1 and take the appropriate actions identified for the physical security features of their facility.

Manufacturer Operating Instructions and Manuals for the physical security features installed in each recruiting facility are to be placed in Attachment C.

4.2.2 Access Control Under Force Protection Conditions

This section identifies the access control requirements for all recruiting facilities under each Force Protection Condition. Higher headquarters notifies all recruiting facilities whenever there is a change to the current Force Protection Condition. The steps or actions that are required for each condition level are identified below.

This information is For Official Use Only (FOUO). It is provided in this draft as a separate handout. Alternatively, it could be incorporated in the manual at this point. We recommend making it a separate handout to keep the entire manual from being FOUO.

4.3 MAIL HANDLING PROCEDURES

This section outlines the mail handling and delivery screening procedures to be followed at all recruiting facilities for letters and packages.

Proper screening and handling procedures for letters and packages are very important. Normally, mail and packages should be separated into two categories: (a) from a familiar or known source, and (b) from an unknown or suspicious source. Although all mail and packages should be screened, mail/packages from known and familiar sources can be routinely handled and distributed. Suspicious mail/packages from unknown sources should be isolated and the addressee or Recruiting Supervisor should be contacted immediately, and a thorough screening, as outlined in the following paragraphs, should be conducted.

A letter and/or parcel bomb, or otherwise contaminated (e.g., anthrax) letter or parcel, is a very serious incident. Careful inspection and screening is an essential component of the security process. For that reason, the following screening procedures for postal and other delivered items should be adhered to and followed as a routine.

4.3.1 Initial Mail Screening

Incoming mail and packages in any organization follows basically the same pattern as described below.

- Bundles or bags of mail, as well as parcels, are delivered to the front door, a centralized mail center or dropped on a desk for distribution (depending on the size of the facility).
- The initial sorting of the mail for delivery to units, divisions, or individuals must be done by hand, with each item being picked up, its address read, and the item is either given to the addressee, put in its proper location, or placed in a distribution box for delivery.
- Initial screening is the point where screening of incoming mail/packages for suspect or suspicious items should occur. All individuals that handle initial mail sorting should perform normal screening actions. See Attachment B 2.
- This is a critical step because those individuals that conduct the initial screening are the most likely persons to notice postal items that are contrary to normal mail, or that may contain an explosive or incendiary device or other contaminate.

4.3.2 Suspicious Mail/Packages

Avoid opening unnecessary mail, such as “junk” mail, or mail from an unidentified or unknown source. Especially avoid opening mail that is suspicious in appearance. Indications of suspicious mail/packages and the steps that should be taken during the initial screening whenever mail/packages are encountered that are considered to be suspicious are outlined in Attachment B 2, *“Initial Screening of Suspicious Mail/Packages.”*

Mail/packages that are suspicious and/or are from an unknown source that has not been opened should be more closely evaluated before opening or discarding in the regular trash. In this situation, refer to and follow the procedures in Attachment B 2, *“Initial Screening of Suspicious Mail/Packages”* identified for *Opening Mail/Packages From An Unknown Source*.

4.4 RECRUITERS AND OPERATIONAL INFORMATION CONTROL

Terrorist operations against informational assets are a growing concern. While the majority of attacks against DoD informational systems have been conducted for monetary gain or "hackers" looking for a thrill, it is possible that terrorists may seize upon this venue for future attacks

4.4.1 General Information Control

The recruiting facility supervisor is responsible to ensure that all personnel follow the following procedures and guidelines regarding general information. The procedures should include the following actions.

- Secure official papers and electronic information from unauthorized viewing.
- Use extreme care when providing information over the telephone. Remember that any and all telephone lines may be tapped.
- Do not give out potential targeting information such as home addresses and phone numbers to people who do not have a bonafide requirement or need-to-know the requested information.

4.4.2 Computers

The recruiting facility supervisor is responsible to ensure that all personnel follow the following procedures and guidelines regarding computer security.

- Use password protection and *do not* post passwords (e.g., sticky notes on or near the computer). The individual having custody and control of the computer and the network administrator are the only individuals that should have access to computer operating system passwords; only the individual having custody and control of the computer should have access to passwords for his/her files
- Do not leave unsecured computers, especially computers that are turned on, unattended where others can access the information.

- Keep the anti-virus programs current and be suspicious of unexpected or suspect attachments. If you are in doubt about the validity of any email or other type of attached file, *do not* open the file until you can verify that it is safe to open through the system administrator or a known sender.
- Control the storage and destruction of official information, e.g., floppy disks, CDs, and memory cards.

4.4.3 Unclassified Information

The DoD has no official definition of Unclassified in DoD Regulation 5200.1-R (Information Security Program Regulation), DoD Manual 5220-22-M (Industrial Security Manual for Safeguarding Classified Information), or DoD Directive 5220.22 (DoD Industrial Security Program). So, in order to better understand this operations procedure, terms used in this document are intended to modify Unclassified.

Unclassified-Unlimited: Approved for public release. This information under the freedom of Information Act may be released to the public.

Unclassified-Limited or Official Use Only: Information exempt from public release by the Freedom of Information Act or other statutory authority.

The recruiting effort exposes you to many individuals and in order to perform your job certain information must be provided to the potential and new recruits. For the purposes of your job, any general information released by official DoD sources is deemed as information that is unclassified and its dissemination is viewed as unlimited. This information can be released to all persons that you come into contact with while in the performance of your duties. The key here is “while in the performance of your duties”. The information discussed with a new recruit is information that is unclassified, but its dissemination is viewed as limited. This information is private information that is between you and the recruit. This information must be maintained as private information, but not under any DoD security classification. This is unclassified information, but limited to discussion only while serving in an official capacity to represent a new recruit. There are nine exemptions where the Freedom of Information Act does not apply. One of these may be commonly encountered in the performance of your recruiting duties:

Personnel, medical files and other similar files that the disclosure of would constitute a clearly unwarranted invasion of personal privacy, e.g., medical condition, marital status, social security number, unlisted home phone number.

Such documents should be marked “FOUO” or “For Official Use Only” in accordance with your security plans. You should take the necessary precautions to preclude access to the information by those who don’t need it for official activities. Don’t display the information publicly, e.g., bulletin boards. Store the materials in accordance with your security plans. When documents are no longer needed, they should be destroyed using a shredder.

4.4.4 Classified Information

Classified information requires special handling and control. If a need to handle classified materials exists, the recruiting facility supervisor must contact your Command immediately for instructions and procedures *prior to* handling or accepting any classified material. Additionally, only personnel possessing a current DoD Security Clearance of the appropriate clearance level (e.g., Confidential, Secret, Top Secret) may handle the classified material. That individual must also have a documented “need-to-know” in order to perform his/her duties before handling and accessing classified material.

4.5 CRIME PREVENTION TACTICS

This section provides guidance regarding crime prevention tactics for all recruiting facilities and personnel. An important key to the safety of all personnel and protection of facilities and equipment is that **prevention of a crime is better than the cure – in-other-words - deter the crime rather than detect the crime.**

The amount of security you need may be difficult to determine and even harder to measure. Total security is probably impossible to obtain, but remember that criminals normally go after the easy targets. If your environment is more secure than other people's environment, then the other people become the more likely victims.

4.5.1 Develop an Awareness of the Environment

Consider this. Start by developing an awareness of your environment. Learn to identify the threats to your security that already exist or may develop. You don't have to look at everything and everyone suspiciously. However, developing security awareness for where you live, work, play, and drive can help you avoid:

- taking unnecessary risks;
- help you identify the areas needing corrective action; and
- prepare you to react if something does happen.

Play the "What if" game. What if I was working late and was confronted by a burglar? What if a fire started, do I know how to escape? If you are trying to gain one thing by reading this procedure, hopefully, that one thing will be to develop sound security awareness within your environment.

4.5.2 Educate Yourself About Risks.

When you pay more attention to your environment, you can identify areas that increase your risk of becoming a crime victim. Just modifying the environment that you work in can eliminate some risks. Other risks can be removed by changing your day-to-day lifestyle, or our habits. As you become aware of things you do which create an unnecessary risk, avoid these practices. As an example, let's say you are working late at the office and you are the only person there. You should lock the door and lower the blinds. Do not advertise that you are alone in the facility.

Risky Behaviors. Here are some risky behaviors which many people practice each and every day. Don't be one of those people. The following is a list of "Do Not's", each of which involves behaviors that create unnecessary risks. Change your physical environment to increase your personal security.

- ***Do Not*** leave the house, vehicle or office without locking the door;

- ***Do Not*** walk through a parking lot or parking garage (especially one without any lights) to your car alone at night;
- ***Do Not*** drive home from work on a secluded road and low on fuel;
- ***Do Not*** retire for the evening without making sure the house is locked up;
- ***Do Not*** work late without locking the office door or closing the blinds;
- ***Do Not*** leave the keys in a vehicle;
- ***Do Not*** leave the garage door open when away from home;
- ***Do Not*** be the last person to leave the office *without* arming the security system;
- ***Do Not*** open the door without first determining who is on the other side;
- ***Do Not*** give details to strangers over the phone, such as “please call back tomorrow because I am only person here right now”.

4.5.3 Keys Components to Security

What is the Key to Security? There is no single magic answer to the security issue. However, there are some key components that will increase your security and the security of your co-workers. These key security components are:

- Awareness
- Education
- Habits
- Precautions

These components are within everyone’s grasp. Each and every individual can make themselves more secure by becoming aware of their environment, changing their environment when possible, and changing how they interact with their environment.

Think about your work space! Boundary walls, doors, fences and gates are your first line of defense against crime. Are you sure they are adequate and in a good state of repair? Do you allow goods to be stacked against a perimeter fence that could be used as a "ladder" for people to easily escape with your property? Doors and windows of business premises are particularly vulnerable and, once inside, a thief can choose his/her method of exit with your property. The recruiting supervisor must ensure that both personnel and property are secure from both the inside and outside.

4.5.4 Locks and Keys.

Good locks are a strong deterrent and can resist many forms of criminal attack. Start by asking yourself these questions:

- Are the locks of your recruiting facility of high quality, fitted correctly and in good working order? If not, report it to your recruiting supervisor or Command.
- Who has copies of the keys to the facility and vehicles, and is there a key control system in use? Good locks are pointless if key security is poor.
- Are the keys to your facility(ies) and vehicles(s) held by non-responsible personnel? If the answer is yes, report it to your recruiting supervisor or Command so that steps can be taken to retrieve the keys or have the locks changed.
- Is there a strict accounting kept on who has the key(s)? If not, notify your recruiting supervisor or Command.
- In case of emergency, do emergency services personnel (e.g., building security, local police, fire department) know who the key-holders are for your premises? If not, the recruiting supervisor for the facility should publish a recall roster to be posted in a conspicuous place or distributed to building security or emergency services personnel. **NOTE.** There have been a few occasions where thieves have posed as police officers and "summoned" the key-holders to the premises under false pretences. The recruiting supervisor should ensure that all personnel are aware of this

fact and advise them to check with the local police or fire station before responding to the facility.

4.5.5 Crime Prevention Checklist

A general checklist pertaining to Crime Prevention Tactics is provided at Attachment B 3. Each facility recruiting supervisor should refer to Attachment B 3 and ensure that the appropriate procedures and actions identified for crime prevention tactics are disseminated to all facility personnel and that any necessary corrective actions are taken or, when appropriate, reported to their Command.

4.6 SURVEILLANCE DETECTION PRACTICES

4.6.1 Introduction

This section outlines standard surveillance detection practices that are to be followed by all recruiting personnel. The recruiting supervisor for each recruiting facility is responsible to ensure that all personnel under his/her supervision are thoroughly familiar with these practices and that these practices are followed.

Criminals and terrorists cannot succeed easily when vigilant personnel surround their targets. The most effective deterrent is for all personnel--not just security forces--to be attentive to their surroundings. Experience has repeatedly shown that potential adversaries abandon their plans or choose different targets when they believe their presence has been detected, even when their hostile intent remains a secret.

The greatest tragedy of terrorist/criminal activity is often revealed during the post event investigations when one or more witnesses are found who say something like, "I saw a person doing [something unusual] near the scene of the event [beforehand], but I didn't think anything about it." If the "unusual behavior" had been reported to the appropriate security personnel, the incident may have been prevented.

All criminal/terrorist events are preceded by recognizable, unusual behavior days, weeks, and sometimes even months before the event. While terrorists/criminals can shield unusual behavior

from security personnel and cameras, they absolutely cannot keep ordinary people and employees from seeing what they are doing.

Many people view terrorism and criminal behavior like a huge black cloud on the horizon that cannot be stopped. Nothing could be further from the truth. Everyone has an important role to play in stopping these activities. This manual will assist recruiting station personnel at every level in detecting, observing, and reporting unusual activity so security personnel/local police can follow up. Remember, when a potential terrorist/criminal comes to your vicinity to plan an action, he/she will likely be unfamiliar with the area and the normal activities that occur there. You know your own workplace or neighborhood very well. You will easily be able to identify unusual activities.

The risk of being a victim of road rage, workplace violence, domestic violence, or ordinary street crime is far greater than the risk of being a victim of a terrorist attack. Although the term “terrorist/criminal” is used throughout this manual, observation skills and reporting techniques will help protect employees from all the risks mentioned above. These techniques have been employed at US Embassies and Consulates worldwide following the bombings Kenya and Tanzania. Everywhere they have been used, there has been notable decrease criminal activity. As of 1 October 2003, there have been no terrorist events where these techniques are in use.

The objective of this manual is to help you detect and report unusual behavior you may see while conducting your normal activities. Use this manual as a guide to sharpen you skills in taking greater notice of your surroundings. As your skill level increases, the comfort level of would be terrorists/criminals will decline sharply. Hopefully, they will decide to go somewhere else.

4.6.2 Simple Counter-Surveillance Techniques

It is a known fact that fairly simple counter-surveillance techniques can discourage all but the most determined or organized terrorist or criminal organizations. The following precautions should be discussed and practiced by all recruiting personnel, especially during times of increased vulnerability to DoD personnel.

- One of the most important practices is to **BE AWARE OF YOUR SURROUNDINGS** and let all know that we are aware of their presence by looking at strangers.

- Do not set patterns. Varying your routes, changing schedules and unpredictable social appearances can disrupt and discourage most surveillance. The criminal will switch their attention to lazier and softer targets.
- If you feel like you are being followed, make quick changes in your route to see if the individual does the same.
- Be able to recognize the individual in the event that you see that person again.
- If you are walking with a friend while in public, it may be a good idea to confront the person following you.
- Above all, unpredictability requires great self-discipline in order to make it second nature.
- Take advantage of any detection systems available, such as video surveillance cameras in the work place and packing lots.
- Advise your supervisor and local law enforcement that you are being followed.

With just a little extra effort and awareness, you can be at least as smart as the bad guy and beat him at his own game. He/She is looking at and watching you; make certain he/she knows that you are looking at and watching him/her.

4.6.3 How Terrorists/Criminals Select a Target or a Victim

Terrorists and criminals often consider many factors when selecting a target or victim. Some of their considerations are listed below.

Terrorists only

- Terrorists select targets that are: highly visible; have a high economic, symbolic, or sentimental value; and their destruction would be highly disruptive. For example, the World Trade Center represented America's economic might.

- The method of attack selected is designed to: generate shock, widespread public fear, leave a severe psychological impact, and attract a great deal of attention to the terrorist group and their cause.

Terrorists and criminals

- There should be a high potential for success
- Security should be lax or easily overcome
- There is little probability that the intended victim will offer significant or unforeseen resistance.
- There should be multiple opportunities for quick escape after the event. Al Qaeda is an exception to this rule. It prefers suicide attacks to prevent possible capture and interrogation.
- Target may be selected on the basis of race, religion, sexual orientation, or politics.

Criminals only

- Target may be selected in a more emotional, impulsive manner.
- Target may be selected because of a real or imagined slight by a spouse or supervisor.
- In the case of road rage, irrational anger is the prevalent force. The victim may only have to be present when the rage explodes.

4.6.4 Potential Targets

The key to defeating terrorists/criminals is to recognize and report unusual behavior that occurs near a potential target. Your facility might be a potential target for a terrorist group if they are looking for a “soft target” that would impact US military personnel. It is far more likely that local criminals including drug addicts and gang members would consider you, your privately owned vehicle, government vehicles, and your facility an easy target for assaults, burglary, and car theft.

Recruiting personnel invariably work long hours outside the “normal workday” observed by surrounding businesses. This affords the potential criminal opportunities to strike when there are fewer people around to either witness his activities or to intervene.

There may convenience stores, banks, liquor stores, and other potential targets near you facility that might attract armed robbers and inadvertently put you or your facility at risk.

4.6.5 What the Terrorist/Criminal Needs to Know

Terrorists and other criminal need to gather information about their target prior to their attack. Some of the types of information they will be trying to gather are:

Operational Security

- Number, location, and training of any local security staff
- Security staff weapons
- Level of overall vigilance by non-security personnel
- Security staff response to alarms/unusual events
- Location, type, and response time of local law enforcement
- Hours of operation
- Access controls

Physical Security

- Nearby security concerns, i.e. banks, off-site video surveillance, schools, hospitals
- Location of on-site security cameras
- Lighting
- Location and type of alarms

- Fences, barriers, and obstacles, and their weak spots
- Rear or emergency entries that may not be controlled properly
- Any entities having unchallenged/uncontrolled access
- Unguarded/unobserved/unlighted areas

Logistical and Strategic Advantages

- Times when alertness, response, and/or visibility is degraded
- Times when the rewards are greatest, (e.g., more people or money present)
- Observation and planning spots
- Primary and alternate escape routes
- Primary and alternate attack sites
- Time required to accomplish event
- Requirements to control the target/victim

4.6.6 Where to Look

Section 3 presented a list of potential targets and Section 4 gave examples of the types of information a terrorist/criminal must collect on their target. Getting this information requires the criminal or terrorist to physically visit the target. Video cameras, binoculars, the Internet, and other technical tools may be useful, but there is no substitute for being “up close and personal” to get the needed data. The attacker is putting his life on the line based on the information he collects. He has to be absolutely certain that his reconnaissance is complete in every detail.

Around every potential target, there is at least one area and possibly more where the would-be-attacker has to physically be in order to get the information he/she needs. This area is called an “Area of Concentration” or a “Red Zone.” Red Zones include ideal places for observing the target, such as a restaurant or library window across from a target, a park bench, bus stop, or

fishing spot. You can identify Red Zones by considering the potential targets in your area and asking yourself “Where would I have to be to collect the information listed in Section 4?”

Specifically, you need to pretend that you are a terrorist, burglar, mugger, or car thief targeting the facility, its personnel, or associated vehicles. Ask yourself the following questions:

- What is the best way to commit this crime?
- Where is the best place to commit this crime?
- How can I avoid being caught while waiting?
- How much time is required to commit this crime?
- How am I going to get away from the crime scene?

Answering the questions above will help you identify Red Zones.

Once they are identified, Red Zones are the areas where you want to focus your observation skills. You need to know the following:

- Who are the people that are almost constantly in the Red Zone?
- Who are the people that periodically pass through the Red Zone?
- What activities normally occur there?
- What unusual activities might periodically occur there?
- How are emergencies or unforeseen events normally handled there?

In short, you need to mentally “own” the Red Zones to the extent that no new folks can enter the Red Zone without it being very obvious to you and your co-workers. By comparing the activities of the new folks against the normal area activity, it will be easy to recognize those who don’t have a valid reason to be there.

NOTE: In addition to mentally “owning the Red Zones”, station security can be greatly enhanced by “walk arounds”. Several times a week at irregular times, every member of the recruiting station needs to walk around the exterior of their facility, nearby buildings, and alleys. Personnel in facilities located within malls or office buildings should walk completely around those structures. Pay particular attention to the presence of homeless folks or vagrants, dumpster areas, areas not regularly seen by security or other tenants, evidence of vandalism, and graffiti. This will give you a better knowledge of who is in your neighborhood, what sort of behaviors are going on, and changes in gang activity that are reflected in graffiti.

Driving around the facility is not an adequate substitute for walking. Walking allows you to see, hear, and smell what is occurring. If this “walk around” is risky, perform them in pairs or threes. Do not put yourself at risk for this activity.

Be certain that all significant information obtained during these “walk arounds” is disseminated to all station personnel.

4.6.7 What to Look For

Users of this manual are not being asked to be James Bond or clairvoyant. You are not to make any assessment about an individual’s intentions. You are not security or intelligence personnel. You are to observe and report unusual behavior, unusual objects, and unusual circumstances at or near a potential target so security personnel can direct further attention to the situation.

Unusual Behavior

You are looking for unusual behaviors that you cannot readily explain at or near a potential target. The potential terrorist/criminal in a Red Zone knows he or she is doing something wrong. He/she will manifest some of the following behaviors:

Personal Signs/Traits

- Nervousness (excessive smoking, pacing, sweating, etc.)
- Avoidance of eye contact

- Fixation on the target
- Facial concealment with dark glasses, hats, scarves, etc.
- Clothing that doesn't fit the area/weather
- Couples who do not demonstrate any sort of interpersonal relationship
- Shielding activities and masking behavior from onlookers, passing police, security personnel, and video cameras
- Wearing the uniform of delivery, postal, or repair people, but do not function as such.

Unusual Activities – Active

- Ignorance of local customs, laws, or idioms
- Use of binoculars, cameras, night vision devices, GPS
- Making notes or sketches of a potential target
- Pacing off or measuring distances
- Looking for a parking space, but never park when they could

Unusual Activities – Passive

- People who apparently have “nothing to do”
- People who remain in place in spite of inclement weather
- Repeated presence in the same location
- Repeated presence at multiple potential targets
- Loitering in areas that locals consider unsafe
- Sitting in vehicles that are apparently broken, but no effort is made to repair them

- Sitting in a parked vehicle for no apparent reason

More Common Crimes

From the introduction, you will remember that Road Rage, Domestic Violence, and Workplace Violence are far more likely than a terrorist attack. As you become more attentive to your surroundings, you will be more likely to notice signs of these more common crimes.

Road rage

- Speeding
- Severe braking
- Unsafe lane changes, weaving, swerving
- Violent or obscene gestures
- Tailgating
- Angry, hard facial expressions

Workplace violence

- Sudden outbursts of anger
- Dissatisfaction with job or a supervisor
- Increasing level of anger
- Decline in work quality
- Domestic violence (this can visit the workplace)

4.6.8 How and What to Report

Your Area Security Coordinator will specify what and how to report. Some types of reports may be submitted in writing, others may be phoned in, and still others should be phoned directly to 911.

When making a verbal report, follow the format specified by your Area Security Coordinator. Be careful to provide all the requested information or a “did not observe” comment for information that you do not have. Regardless of whether or not a verbal/telephone report has been given, the details of every observation should be written down as soon as possible, while they are fresh in your mind.

A mnemonic such as “ALT-DD” may be useful in remembering what to look for.

ALT – DD

- Activity
- Location
- Time
- Date
- Description

Descriptions are for people and any vehicles associated with them. Reports will always have at least one description of a person including:

- Sex
- Race
- Age
- Height

- Weight
- Complexion
- Distinguishing features

Vehicle descriptions include the following:

- Color
- Make/model
- Year
- Type
- Number of doors
- Distinguishing features
- License number and state

Be aware that license plates are among the easiest things to change, obscure, or steal. Thus, it is important for vehicle descriptions to include features that are more difficult to change.

A disposable camera is always useful to quickly record a person or vehicle, but it should not be used in lieu of a verbal description. Timeliness, completeness, and accuracy are critical factors in reporting.

Report only what you are certain you saw. Add any guesses or impressions at the bottom of the report as a comment. Clarity can be enhanced with the following:

- Nouns, not pronouns (i.e., avoid “he”, “she”, “they”, “it”)
- Provide details
- Write short sentences

- Include only observations, not assumptions.

For example, it is better to write “Person 1 constantly looked towards the front gate. At 3PM, Person 1 left and the empty place was taken by Person 2, who also constantly looked towards the front gate,” rather than “Person 1 constantly watched the front gate. At 3PM, Person 2 replaced him, and did the same thing.” The assumptions, guesses, and intuitive notes such as the gate was being “watched” and that one person “replaced” another should be noted in the comment section rather than as an observation description.

Other types of observations you should report consistent with your Area Security Coordinator’s policy include:

- Loss/theft of ID’s, uniforms, vehicles, official decals, license plates
- Loss of keys, keycards, or key codes
- Any increase in false alarms on the security system
- Indicators of Domestic Violence
- Indicators of a pending Workplace Violence incident
- All observations of Road Rage

Will you make some ridiculous, useless reports? Absolutely!! Everyone practicing these skills makes ridiculous reports. After you have done it for 10 years, you will still make mistakes, but they will be fewer and much more sophisticated.

All reports will be put into a database. The database will, over time, eliminate reports that are not useful. It will identify areas where your Area Security Coordinator may want you to direct more attention. Your reports will create a vigilant atmosphere that will cause potential terrorists/criminals to pick another target. Your reports on incidents potentially involving more common crimes may well save the lives of coworkers as well as your own.

4.6.9 Area Security Coordinator

The recruiting command must appoint an Area Security Coordinator to establish and maintain an effective link between the recruiting stations of all services within a jurisdiction and the local law enforcement agency for that jurisdiction. This individual should be either a senior NCO or an officer with 1 or 2 assistants to afford continuity and responsiveness 24-7. **This does not mean that the office must be open 24-7. It means that a recruiter working at midnight Saturday who observes suspicious activity has someone to whom he can report who can make a decision on how to respond to the report.**

The Area Security Coordinator has the following functions:

- Establishes and maintains liaison and rapport with local law enforcement
- Establishes and maintains liaison with all Area Security Coordinators in adjacent jurisdictions
- Shares relevant reports with adjacent Area Security Coordinators
- Shares relevant reports with recruiting personnel in the local jurisdiction
- Receives all suspicious activity reports from all services within the jurisdiction.
- Maintains a database of all reports
- Screens all reports
- Refers reports to designated law enforcement office as appropriate
- Provides feedback and guidance on reporting to recruiting personnel within the jurisdiction

Local police will most likely be the security force for your area. Generally they are overworked with little time to respond to all but the most serious incidents. On the other hand, all police departments appreciate the assistance of trained observers who do not waste police time and resources. If a report is intelligently prepared, screened by an experienced and accountable

person, and presented in a timely manner to the appropriate supervisor, the police will usually give it a higher priority. Whenever possible, reporting should be done without the 911 system.

4.6.10 When to Intervene

Your Area Security Coordinator will specify when you should intervene and when you should call 911 directly. Generally, you are NOT to intervene. Your steps of action should include:

- Stay safe, alert, and maintain communication
- Do not jeopardize the safety of others
- Make an accurate and timely written report (with photo if possible) ASAP even if a verbal report has already been made

Eminent loss of life is a reason to sound an alarm, try to move people to safer areas, and shutdown building HVAC systems if applicable. Do not jeopardize your own safety.

4.6.11 Potential Actions to Further Improve Security

Skill maintenance:

- Knowing what is normal
- Systematic observation
- Personal awareness
- Do not assume “everything is OK”

4.6.12 Sample Report

Your Area Security Coordinator should provide you with forms for reporting unusual observations. An example of the type of information that should be in this form is shown as Attachment B 9.

4.6.13 A Few Key Reminders

Do not overlook the following:

- Couples, especially those not demonstrating a relationship with each other
- Handicapped
- Children
- Homeless
- Beggars
- Women
- Folks with babies or strollers
- Repairmen/service personnel
- Delivery people
- Bicyclers/joggers
- Fishermen
- Drivers with broken down vehicles
- Vehicles with obscured or missing license plates

4.6.14 Protecting Yourself Against Stalkers/Stalking

In recent years, society has become more aware of the dangers of stalking. Stalking, under most state laws, is repeated harassment that could or does cause the victim to feel intimidated, threatened or frightened. While it is difficult to prevent stalking from occurring, you can take steps to prevent it from continuing.

- If you are a victim of stalking, report it to your recruiting supervisor and the local police department, even if you do not know whether or not you will be filing charges.
- Gather information to help your case, such as taped recordings of threatening phone calls, license plate state and number, description of vehicle, a description of the individual(s), and a detailed listing of any contacts the stalker makes with you.
- Follow up in court. Take out an anti-stalking order at your local circuit court and/or file a civil lawsuit against the stalker for damages resulting from the stalker's behavior.
- If the stalking continues after the anti-stalking order has been sent, contact the police.
- If you think that you are being stalked, ensure that someone (e.g., your recruiting supervisor) is aware of your schedule, location and anticipated routes of travel for the day prior to leaving the office.

No method of crime prevention is guaranteed to work 100% of the time. However, in taking these steps, you are removing opportunity from would be criminals, and you will be less likely to be victimized. Be smart. Learn these steps and make them a habit in your life.

4.7 PROCEDURES FOR SPECIAL ACTIVITIES

Site selection for setting up future recruiting facilities at special activities is extremely important from both a security aspect and from a successful recruiting aspect. The significant security advantages that can be gained by setting up the temporary recruiting location within the “secure area” of a special activity are obvious. Recruiters also need to select highly visible locations to enhance their mission while maintaining a constant vigilance for potential dangers.

The following procedures are recommended and should be followed by all recruiting personnel engaged in recruiting activities at special events.

4.7.1 Planning and Preparation Procedures

- Plan activities and security needs ahead of time.
- Ensure that you know the special event site and surrounding area.
- Involve the ATO in planning and implementation.
- Take advantage of existing “event security” whenever possible:
 - Coordinate with event security personnel and local authorities
 - Whenever possible, discuss your security plan with Event Security Staff to ensure it will not be a cause for any issues, and try to obtain a general understanding of their Security Plan for the event
 - Discuss Event Site set-up with Event staff and try to obtain a set up location for the recruiting effort that will take advantage of event security while maximizing exposure to the public whenever possible
- The recruiting supervisor for the special event should reinforce awareness and procedures with all involved recruiting personnel prior to the event.
- Plan for vehicle access and security.

4.7.2 General Security

- Guard information that could be used for targeting by:
 - Limiting discussion and accessibility of any information (written or verbal) that may provide terrorists or criminals insights for targeting
 - Always using caution when you need to pass sensitive information on to other involved personnel. Use a secure means of communication, if possible.
- Recognize and Report Unusual or Suspicious Behavior

- YOU ARE THE FIRST LINE OF DEFENSE AGAINST TERRORISM AND CRIMINALS. Be aware of your surroundings. Report anything unusual to your recruiting supervisor or Command, as appropriate.
- Write down license plate numbers of suspicious vehicles and note descriptions of occupants.
- Be prepared for the unexpected.
 - Plan for the range of threat possibilities.
 - Avoid established or predictable patterns.

4.7.3 Vehicle Security

- Never leave unsecured vehicles unobserved or vulnerable for easy attack. Government recruiting vehicles are easily identifiable and often targets of terrorists and criminals.
- Look for tampering. Always look under, in and around your vehicle for signs of tampering before entering the vehicle if it has been left unattended. If signs of tampering are identified, notify your recruiting supervisor and local police immediately.
- Never leave keys in your vehicle and keep all windows closed and doors locked when the vehicle is left unattended.

4.8 REPORTING REQUIREMENTS

This section summarizes the reporting requirements for personnel at military recruiting facilities for terrorist and criminal activities.

4.8.1 Medical Emergency

In a medical emergency, call 911 immediately and request emergency medical assistance. Next, notify your recruiting supervisor and Command emergency point of contact.

4.8.2 Suspicious Activity

The simple act of recognizing and reporting suspicious activities or behavior can thwart terrorist and criminal acts and save lives. Be alert and report any suspicious activity to your recruiting supervisor and Command. This includes suspected hostile surveillance and suspicious persons who seem to be out of place. If you suspect that the suspicious activity is terrorist related, also notify the ATO.

4.8.3 Contact Numbers

A Point of Contact List containing the names and numbers of individuals, emergency response personnel, agencies and others as necessary is located at Attachment A of this manual. Refer to Attachment A for the appropriate contact numbers.

Call 911 for emergency response personnel, such as ambulance, police or fire. Other individuals/agencies that may need to be notified (depending on the situation) could include:

- Ambulance.
- Your recruiting supervisor.
- Your Recruiting Command Headquarters.
- The Command Anti-Terrorism Officer (ATO).
- Local Air Force, Army, Navy or Marine Corps recruiting personnel.
- The Center for Disease Control (CDC).
- Facility Maintenance.
- Fire Department/ Fire Protection.

- Hospital Emergency
- Local Law Enforcement (Police, Sheriff, Highway Patrol or State Police).
- Monitored Alarm Services Company.
- Poison Control Center.
- Rescue Squad.
- Building Security
- Utilities (electric, gas, water, phone)
- Local Federal Bureau of Investigation (FBI) Office.

4.8.4 Utility Failures

In the event of utility failure, the following actions and procedures should be followed. All phone numbers for notifications are listed in Attachment A.

- Call the building maintenance custodian. If there are no building maintenance personnel for your facility, contact the appropriate individual at your Command.
- Use flashlights if electrical power is disrupted.
- Turn off all electrical, office, and computer equipment. Some equipment, if left on, could be damaged when power is restored. **DO NOT UNPLUG YOUR TELEPHONE!**
- Remain in your area if power loss is not related to another emergency condition, such as smoke or fire. Continue routine assignments where feasible and await further instructions.
- Re-check equipment after power is restored.

- You may be instructed to contact appropriate utility maintenance personnel directly. Routine and emergency phone numbers for electrical, gas and water utilities are provided in Attachment A.
- For routine telephone repairs, call the number listed in the local phone book under repairs, or call the operator.
- In the unlikely event of a system-wide failure of the telephone system:
- You should call the telephone repair number from a cellular telephone or a local pay phone.
- If an emergency of another nature exists, call 911 from a cell phone for emergency assistance.
- If the telephone company is experiencing a major failure, information about the failure and other pertinent messages will be made by radio and TV announcements.

4.9 VEHICLE SECURITY PROCEDURES

Vehicles left in parking lots, parked on the street, at Automatic Teller Machines (ATMs) and social events always present a target for thieves and the potential for personal assault and/or car jacking. The following steps can help lessen the chance that the recruiting vehicle, property in the vehicle, or you will be a victim of a criminal act.

4.9.1 Vehicle Security Precautions

All recruiting personnel responsible for recruiting vehicles should adhere to the following precautions. It is also suggested that these precautions be followed for your own privately owned vehicle (POV).

- Park in well-lighted, well-traveled areas.
- Do not leave expensive property, such as CD cases, purses, radar detectors, cellular phones and portable stereos in plain view in your car. Lock them in your trunk or

take them with you when parking the vehicle. Cover up conspicuous stereo equipment, if possible. Remember that thieves target after-market stereo equipment, not factory installed equipment.

- Lock your vehicle and close all windows.
- Never leave items visible inside your vehicle.
- Never store or hide spare keys in or on your vehicle.
- Record the brand, model numbers and serial numbers of all electronic equipment installed in the vehicle. In the event of theft, give this information to the police. If the equipment is recovered it can then be returned to you. Also engrave your driver's license number on any of this equipment that is personally owned.
- Most fairly new vehicles come with a factory installed alarm system. It is recommended that the applicable Recruiting Command consider checking with the Government Services Administration (GSA) motor pool regarding installation of an aftermarket vehicle alarm system for vehicles without an alarm system, especially for vehicles located in high crime areas.
- For POVs, it is suggested that you engrave your Vehicle Identification Number (found on your registration or under the windshield on the driver's side) on the doors, windows, fenders and trunk lids of your car. This engraving would need to be pre-approved through the applicable Recruiting Command and GSA Motor Pool prior to implementation. This will prevent theft because the thief would need to replace these parts before selling the car.
- If available, use a steering wheel lock when the vehicle is parked. While these devices can be defeated, a thief may decide it's not worth the effort.
- Conduct a search of the area immediately adjacent to, under and in the vehicle any time the vehicle has been left parked outside and unattended over night prior to using the vehicle. Refer to Attachment B 4.

4.9.2 Vehicle Security at ATMs

In recent years, ATMs and their users have become a target for thieves. In today's society, most ATMs are accessed via drive-thru ATM machines and, therefore, individuals using ATMs are most often in their vehicle. Here are some tips you should know to prevent yourself from becoming a victim at an ATM:

- If at all possible, avoid using ATMs at night. If you must use one at night, select one with a lot of people around that is well lighted and is not in a secluded, low visibility area.
- Try to have a friend accompany you when using an ATM.
- Be aware of your surroundings and the people around you.
- While approaching, leaving and at an ATM drive-thru machine, ensure that all vehicle doors are locked and that all windows except the driver's door window are fully closed. The driver's window should not be open any further than necessary to access the ATM.
- Complete your transaction as quickly as possible, depart the area as soon as the transaction is completed, and do not flaunt your cash.

4.9.3 Protecting Yourself Against Sexual Assault

If you are being victimized by a person who is attempting to sexually assault you while you are in a vehicle, take the following steps to stop the assault from progressing. Remember that the goal is survival.

- If necessary, stall for time and figure out your options. Each situation is different. Decide if you will flee the area, try to escape from the vehicle, fight, try to talk your way out of the assault, scream, or, if necessary for your survival, submit.

- If outside the vehicle, you will need to determine whether you should flee on foot or try to get in the vehicle (if the assailant(s) is outside the vehicle), lock the doors and flee in the vehicle.
- In some situations (e.g., you are in the vehicle, the assailant is outside, the vehicle is running and you fear for your life) you may have to decide to hit/run down the assailant or assailants in order to save yourself.
- If you have to fight, hit hard and fast. Target the eyes and groin.
- You may decide to try to dissuade the attacker from continuing. In this situation, tell him you have a sexually transmitted disease or that you are menstruating, urinate, vomit, or do/say anything to else to discourage the attacker from continuing.
- If all else fails and you are in fear for your life, you may determine that your best option is to submit.

4.10 PHYSICAL SECURITY EQUIPMENT

As previously stated in paragraph 4.2.1, each recruiting facility will have physical security hardware installed based upon the facility type, location, construction, and lease agreements. General responsibilities and procedures for physical security features are described in Attachment B 1. Manufacturers and/or vendors Operating Instructions, Operating Manuals and Owner's Manuals will be provided to each facility for the physical security hardware/equipment installed at that facility. These instructions and manuals are to be located in Attachment C of the copy of this OSM for the specific facility.

It will be the responsibility of the recruiting supervisor of each facility to ensure that copies of Operating Instructions, Operating Manuals and Owner's Manuals are obtained and placed in Attachment C for hardware/equipment that is installed at a later date.

5.0 EMERGENCY MEDICAL PLANS AND CBRNE PLANS

This Section addresses Medical Plans and Chemical, Biological, Radiation, Nuclear and Explosives (CBRNE) Plans.

5.1 MEDICAL PLANS AND CONTACT INFORMATION

A medical emergency is any situation - actual or imminent - that endangers the safety and/or lives of personnel and the general public. A plan should be in place to deal with medical emergencies and all recruiting personnel and staff need to be familiar with this plan in order to respond appropriately in case of a medical emergency. The general guidelines and procedures for a medical emergency are outlined below. It is the responsibility of the recruiting supervisor to ensure that all personnel are cognizant of the plan and to ensure that emergency phone numbers are kept up to date. Refer to Attachment A.

Additionally, ensure that all personnel at each facility are aware of who within the facility is trained and certified to administer First Aid and CPR. A list should be maintained by the recruiting supervisor for each facility and posted in a conspicuous place that includes the names, telephone numbers of trained and certified personnel. This list should also identify whether they are certified to administer First Aid, CPR, or both and the expiration date of their certification.

5.1.1 Emergency Telephone Numbers

For immediate assistance in a medical or safety emergency, **call 911**. Other emergency numbers, such as the local ambulance, hospital emergency room, air med-evac, fire department, etc. are listed in Attachment A, Point-of-Contact List.

When you call for emergency support in a medical emergency, be prepared to provide the following information:

- Identify yourself and the specific location (e.g. street address, suite, exact location within a mall or large office building) of the emergency.
- Explain what has occurred. Be concise and factual.

- Relate known or suspected injuries or fatalities.
- Identify immediate help needed.
- If known, identify any specific medical conditions of the persons involved, such as diabetes, high blood pressure, allergies, etc.
- Ask if there is anything you should do for the victim while awaiting help.

5.1.2 Emergency Actions

In the event of an injury or other medical emergency, you should:

- Request emergency medical support, as outlined above
- Obtain or provide on-site first aid.
- Alert other personnel/visitors that an emergency is occurring.

5.2 CHEMICAL, BIOLOGICAL, RADIATION, NUCLEAR, AND EXPLOSIVE (CBRNE) PLANS AND INFORMATION

This section provides plans, information, and procedures relating to a chemical, biological, nuclear/radiological, and/or explosive (CBRNE) event.

5.2.1 Hazards From CBRNE Attacks

The hazard from a chemical, biological, nuclear/radiological, and/or explosive (CBRNE) event is always present. However, the detection of such attack, in most cases, will not be readily recognized until the attack occurs. Active duty personnel as well as civilian workers in government facilities should be familiar with identifying unusual symptoms, patterns of symptom occurrence, and any additional cases of symptoms as the effects spread throughout the community and beyond. For the purposes of this discussion, let's start with explosives because is probably the most commonly used, most readily available and also used as the expulsion charge for other hazardous items.

Chemical. Chemical agents are intended to kill, seriously injure, or incapacitate people through physiological effects. A terrorist incident involving a chemical agent will demand immediate reaction from emergency responders—fire departments, police, hazardous materials teams, emergency medical services, and emergency room staff—who will need adequate training and equipment. Hazardous chemicals, including industrial chemicals and agents, can be introduced via aerosol devices (e.g., munitions, sprayers, or aerosol generators), breaking containers, or covert dissemination. Such an attack might involve the release of a chemical warfare agent, such as a nerve or blister agent or an industrial chemical, which may have serious consequences. Some indicators of the possible use of chemical agents are listed below.

Early into an event, it may not be obvious whether an outbreak was caused by an infectious agent or a hazardous chemical; however, most chemical attacks will be localized, and their effects will be evident within a few minutes. There are both persistent and non-persistent chemical agents. Persistent agents remain in the affected area for hours, days, or weeks. Non-persistent agents have high evaporation rates, are lighter than air, and disperse rapidly, thereby losing their ability to cause casualties after 10 to 15 minutes, although they may be more persistent in small, unventilated areas. Most chemical attacks have the following general indicators of possible chemical agent use.

- Unusual Occurrence of Dead or Dying Animals. For example, lack of insects, dead birds
- Unexplained Casualties.
 - Multiple victims
 - Surge of similar 911 calls
 - Serious illnesses
 - Nausea, disorientation, difficulty breathing, or convulsions
 - Definite casualty patterns

- Unusual Liquid, Spray, or Vapor
 - Droplets, oily film
 - Unexplained odor
 - Low-lying clouds/fog unrelated to weather
- Suspicious Devices or Packages
- Unusual metal debris
- Abandoned spray devices

Biological. Recognition of a biological hazard can occur through several methods, including identification of a credible threat, discovery of bio-terrorism evidence (devices, agent, clandestine lab), diagnosis (identification of a disease caused by an agent identified as a possible bio-terrorism agent), and detection (gathering and interpretation of public health surveillance data).

When people are exposed to a pathogen such as anthrax or smallpox, they may not know that they have been exposed, and those who are infected, or subsequently become infected, may not feel sick for some time. This delay between exposure and onset of illness, or incubation period, is characteristic of infectious diseases. The incubation period may range from several hours to a few weeks, depending on the exposure and pathogen. Unlike acute incidents involving explosives or some hazardous chemicals, the initial response to a biological attack is likely to be made by direct patient care providers and the public health community.

Terrorists could also employ a biological agent that would affect agricultural commodities over a large area (e.g., wheat rust or a virus affecting livestock), potentially devastating the local or even national economy. The response to agricultural bio-terrorism should also be considered during the planning process.

Responders should be familiar with the characteristics of the biological agents of greatest concern for use in a bio-terrorism event. Unlike victims of exposure to chemical or radiological

agents, victims of biological agent attack may serve as carriers of the disease with the capability of infecting others (e.g., smallpox, plague). Some indicators of biological attack are provided below.

- Unusual Occurrence of Dead or Dying Animals
- Unusual Casualties
 - Unusual illness for region/area
 - Definite pattern inconsistent with natural disease
- Unusual Liquid, Spray, or Vapor
- Spraying and suspicious devices or packages

Nuclear/Radiological. The difficulty of responding to a nuclear or radiological incident is compounded by the nature of radiation itself. In an explosion, the fact that radioactive material was involved may or may not be obvious, depending upon the nature of the explosive device used. Unless confirmed by radiological detection equipment, the presence of a radiation hazard is difficult to ascertain. Although many detection devices exist, most are designed to detect specific types and levels of radiation and may not be appropriate for measuring or ruling out the presence of radiological hazards. Some general indicators of Nuclear Weapon/Radiological Agent use are listed below.

- A stated threat to deploy a nuclear or radiological device
- The presence of nuclear or radiological equipment (e.g., spent fuel canisters or nuclear transport vehicles)
- Nuclear placards or warning materials along with otherwise unexplained casualties

Scenarios Constituting Intentional Nuclear/Radiological Emergency. The scenarios constituting an intentional nuclear/radiological emergency might include the following:

- Use of an Improvised Nuclear Device (IND) includes any explosive device designed to cause a nuclear yield. Depending upon the type of trigger device used, either uranium or plutonium isotopes can fuel these devices. While “weapons-grade” material increases the efficiency of a given device, materials of less than weapons grade can still be used.
- Use of a Radiological Dispersal Device (RDD) includes any explosive device used to spread radioactive material upon detonation. Any Improvised Explosive Device (IED) could be used by placing it in close proximity to radioactive material.
- Use of a Simple RDD that spreads radiological material without the use of an explosive. Any nuclear material (including medical isotopes or waste) can be used in this manner.

Conventional Explosive Devices. The easiest to obtain and use of all weapons is still a conventional explosive device, or improvised bomb, which may be used to cause massive local destruction or to disperse chemical, biological, or radiological agents. The components are readily available, as are detailed instructions to construct such a device. Improvised explosive devices are categorized as being explosive or incendiary, employing high or low filler explosive materials to explode and/or cause fires. Bombs and firebombs are cheap and easily constructed, involve low technology, and are the terrorist weapon most likely to be encountered. Large, powerful devices can be outfitted with timed or remotely triggered detonators and can be designed to be activated by light, pressure, movement, or radio transmission. The potential exists for single or multiple bombing incidents in single or multiple municipalities. Historically, less than 5% of actual or attempted bombings were preceded by a threat. Explosive materials can be employed covertly with little signature, and are not readily detectable. Secondary devices and booby traps may also be in conjunction with explosive devices and targeted against emergency responders. The explosives event will be instant and the damage will vary from total destruction to areas that are essentially undamaged as compared to others areas or structures. The loss of life is usually instant in the vicinity of an explosion with varying degrees of injuries from flying debris such as building materials, shards of glass and other materials. The heat and blast pressures associated with an explosion are tremendous, sometimes in excess of 5,000

degrees with over-pressures exceeding 10,000 pounds per square inch. In the case of an attack using chemicals, biological agents or radiological contamination, a small explosive charge is normally the medium for dispersal of such contaminants. The detection of a terrorism incident involving biological agents (as well as some chemical agents) will most likely occur through the recognition of the symptoms by alert medical technicians. Detection of some biological, chemical and radiological agents could occur days or weeks after exposed individuals have left the site of the release.

Combined Hazards of CBRNE. Chemical, biological and radiological agents can be combined to achieve a synergistic effect, greater in total effect than the sum of their individual effects. They may be combined to achieve both immediate and delayed consequences. Mixed infections or intoxications may occur, thereby complicating or delaying diagnosis. Casualties of multiple agents may exist; casualties may also suffer from multiple effects, such as trauma and burns from an explosion, which will only worsen the likelihood of chemical agent contamination. Attacks may be planned and executed so as to take advantage of the reduced effectiveness of protective measures produced by employment of an initial WMD agent. Finally, the potential exists for multiple incidents in single or multiple areas.

5.3 PREVENTION AND ACTIONS BEFORE ANY EVENT

- Report anything unusual or suspicious such as out of place vehicles, packages, people, strange smells, powders, liquids, clouds, a group of people with similar medical symptoms, etc. to your commander and ATO.
- Prepare and review response plans

5.3.1 Actions if Attack is Expected

- Contact command and the ATO
- Harden the facility; e.g., shut down ventilation, control access
- Review general response plans

5.3.2 Actions During an Event

- Listen to the instructions offered by all Emergency Responders, Security, Safety, and Facilities personnel.
- Stay calm.
- Evaluate the situation. Evacuation may not always be the safest course of action. If you evacuate at the wrong time, it may make the situation worse. You may be instructed to remain in your office and keep all doors and windows closed. If you run without knowledge or direction, you may run directly into the danger area.
- You may be told to take one of three actions, depending on the situation:
 - Shelter-in-place
 - Internal relocation (move to another part of the building)
 - Evacuate

5.3.3 Actions After the Event

- Contact command. Contact medical and other response teams as needed.
- Do not go anywhere else unless directed to do so. If you do, you may spread contamination and hurt other people. You need to stay where trained help can render aid and assistance.
- You may need to self-decontaminate: Do it only if you believe you have been contaminated.
 - Move away from the contaminated area
 - Remove contaminated clothing
 - Wash thoroughly with soap and water

- Fireman or other responders may have the ability to determine who needs full decontamination.
- If a biological agent is used, you may receive medicine or immunizations.
- Account for people who were exposed to the attack.

6.0 LOCAL EMERGENCY SERVICES GUIDANCE

This section will outline bomb threat procedures, a fire protection program, civil disturbances and protests, and disaster and emergency plans. All recruiting personnel should be thoroughly familiar with the contents of this section, the procedures to be followed in the event of an emergency, and the applicable checklists provided in Attachment B.

The recruiting supervisor for each recruiting facility is responsible to ensure that all assigned personnel understand these procedures and are trained to take the actions necessary in the event that local emergency services are required.

6.1 BOMB THREAT PROCEDURES

The following **EMERGENCY ACTIONS** are to be taken **WHEN A BOMB THREAT IS RECEIVED BY PHONE**:

- If the threat of explosion is immediate, evacuate all people from the premises at once.
- If the caller indicates there's some time before the bomb will go off:
 - Try to get as much information as possible about the location and description of the bomb, and the caller. Use the BOMB THREAT CHECKLIST (see Attachment B 5) to record all information and *take the checklist with you when you leave the building.*
 - Stay on the line only as long as the caller continues to provide useful information.
 - Immediately evacuate the premises. Take the checklist with you.
- Call 911 and request police and bomb squad emergency assistance. Provide 911 operator the above information.
- All bomb threats and warnings received by telephone or mail should be reported immediately.

- Notify the facility supervisor, appropriate Command personnel, and building maintenance personnel (when applicable).
- Keep all personnel away from the facility or area until emergency response personnel arrives.
- Do not re-enter the facility or area until the area has been declared “safe” by appropriate emergency response personnel.

The following **EMERGENCY ACTIONS** are to be taken upon **discovery of a bomb or suspicious item**.

- If you find an item you suspect is a bomb, **DO NOT** touch, move or disturb the item under any circumstances.
- Call 911 immediately.
- Evacuate all personnel from the area.
- Notify the facility supervisor, appropriate Command personnel, and building maintenance personnel (when applicable).
- Keep all personnel away from the facility or area until emergency response personnel arrives.
- Do not re-enter the facility or area until the area has been declared “safe” by appropriate emergency response personnel.

6.2 FIRE PROTECTION PROGRAM

It is important that all personnel know the type and location of all fire emergency resources in their area and for their facility. Additionally, the recruiting supervisor for each facility should ensure that a facility evacuation plan is posted conspicuously at appropriate locations throughout the facility and that a pre-established assembly point is established for evacuation purposes.

Each individual should know where the following types of fire emergency resources are located for their facility.

- Fire alarm pull stations
- Fire extinguishers
- Fire Hydrants
- Fire exits
- Sprinkler systems

EMERGENCY ACTIONS that are to be followed if a fire occurs or you detect smoke or a burning odor are located at Attachment B 6. The recruiting supervisor should ensure that all personnel are thoroughly familiar with the emergency actions identified.

Fire emergency resources within a recruiting facility need to be properly functioning at all times. In most areas, fire extinguishers, fire hydrants, pull boxes and sprinkler systems are periodically inspected by fire department personnel. If you are notified that any of these devices are not functioning properly or need to be filled, it is your responsibility to notify your supervisor, the appropriate individual at your Command, or building maintenance personnel and request that necessary repairs be made or that empty fire extinguishers are filled or replaced. The recruiting supervisor should ensure that emergency exit lights and door panic bars are functioning properly and that fire exits are not blocked. If emergency exit lights or panic bars are not functioning properly, building maintenance personnel or the appropriate individual at your Command should be notified so that they can ensure that the necessary maintenance or repairs are made.

6.3 CIVIL DISTURBANCES AND PROTESTS

Most demonstrations such as marches, meetings, picketing and rallies will be peaceful and non-obstructive. A demonstration should not be disrupted unless one or more of the following conditions exists as a result of the demonstration:

- **INTERFERENCE** with the normal operations of the Facility.

- PREVENTION of access to office, buildings, vehicles or other recruiting property.
- THREAT of physical harm to personnel or damage to recruiting facilities.

If any of these conditions exist, the Police should be notified immediately and you are be responsible for notifying your recruiting supervisor or the appropriate individual at your Command.

Depending on the nature of the demonstration the appropriate procedures listed below should be followed:

Peaceful, Non-Obstructive Demonstrations. Generally, demonstrations of this kind should not be interrupted, obstructed or provoked in any manner, and efforts should be made to conduct business as normally as possible.

If demonstrators are asked to leave, but refuse to leave by regular closing time:

- Arrangements will should be made for the Police to monitor the situation during non-business hours, or
- A determination may be made by the Police to treat the violation of regular closing hours as a disruptive demonstration and take appropriate.

Non-Violent, Disruptive Demonstrations. In the event that a demonstration blocks access to the recruiting office or interferes with the operation of the facility in violation of the laws for conducting demonstrations, the following guidelines should be followed.

- If the demonstrators persist in the disruptive activity, they are to be notified that failure to discontinue the specified action within a determined length of time may result in intervention by civil authorities.
- If a determination is made to seek an intervention by the Police, the demonstrators should be so informed. Upon arrival of Police and/or other law enforcement personnel, demonstrators remaining in the area will be dealt with by the police.

- Notify your supervisor and the appropriate individual(s) at your Command.
- Efforts should be made to obtain positive identification of demonstrators in violation in order to facilitate later testimony, including photographs and/or videotaping, as long as you can do so without placing yourself or other recruiting personnel in any danger.

Violent, Disruptive Demonstrations. In the event that a violent demonstration in which injury to persons or property occurs or appears imminent, call 911 or the Police and notify them of the situation and request emergency support immediately. The police will assist in removing personnel from the facility and secure the area. Also, notify your supervisor and the appropriate individual(s) at your Command.

6.4 DISASTER AND EMERGENCY PLANS

6.4.1 Severe Weather/Tornado

This section is devoted to procedures that should be followed in the event of these severe weather conditions.

EMERGENCY ACTIONS - Should threatening weather conditions develop:

- Use your location's weather alert radio or television weather channel to monitor the approach and severity of the weather:
 - Tornado Watch means weather conditions are favorable to the formation of tornadoes.
 - Tornado Warning means a tornado has been sighted in the area.
- If the Weather Service issues a severe weather or tornado warning for the area, warn employees in your immediate area.
- Close all doors; stay away from windows.

- Employees should move to a pre-planned shelter and make a headcount.
- If available, take a battery-powered radio and a flashlight into the shelter.
- Remain in the shelter until an all-clear is given.
- Reconvene employees when the emergency is past to make sure everyone is safe.
- Report any damage to your recruiting supervisor or Command.

SHELTERS – The best areas to seek shelter in are:

- basement
- inside walls on opposite side of corridor from which storm is approaching
- restrooms without windows
- interior hallway on lowest or ground floor (no windows, doors secured at either end)

The following should be avoided:

- lobbies
- walkways
- atriums
- rooms with large roof spans, such as auditoriums
- end rooms in one-story buildings
- rooms with large glass areas
- hallways that could become "wind tunnels"

If you are driving a car in open country, do not attempt to drive out of the way of a tornado. Tornadoes are very unpredictable in their movements. *Get out of your car and lie flat in the nearest ditch or ravine, face down with hands over the back of your head.*

Additionally, you should:

- Monitor approaching storm conditions - freezing rain, sleet, heavy snow, sustained high winds, wind-chill conditions.
- Ensure that all personnel are aware of cold weather safety rules and understand Command policy for operating or closing recruiting facilities under adverse weather conditions.

6.4.2 Floods

- In heavy rains, be aware of flash floods. If you see any possibility of a flash flood occurring, move immediately to a safer location.
- Monitor reports on flood conditions. If advised to evacuate:
 - Secure the building.
 - Lock the doors and windows.
 - Calmly leave immediately.

6.4.3 Lightning

- When a thunderstorm threatens, go inside immediately for protection.
- When indoors, stay away from windows, water, sinks and faucets.
- If you are in a hard-topped car, stay there.
- If you are caught outside, stay away from any object that could act as a natural lightning rod, such as a tall tree in an open area. Stay clear of open fields, open water or small isolated sheds. *If you are caught in a field, crouch low to the ground; do not lie flat on the ground.*
- Get away from fences or other metal objects.

6.4.4 Utility Failure

Refer to Section 4.8.4 of this manual.

6.4.5 Chemical Spills

Inside Of The Recruiting Center. It is the responsibility of the facility supervisor to know the characteristics of any chemicals that are in the vicinity of the workplace and to take precautions to protect themselves and the public from an unintentional exposure by containing spills that may occur.

Within Your Work Area. It is the responsibility of employees to know the characteristics of the chemicals that they work with and to take precautions to protect themselves and others by containing spills that may occur.

Emergency Actions For Any Chemical Spill. Refer to the checklist located at Attachment B 7.

General Cleanup Procedure - For Minor Spills Only. Follow these procedures for cleanup of minor spills:

- Only trained personnel should attempt to clean up spills. Cleaning up chemical spills is dangerous and should only be performed by professionally trained persons.
- Clear all persons out of the area who are not directly involved in the cleanup.
- Obtain an Material Safety Data Sheet (MSDS) for the chemical that was spilled. Follow all safety precautions identified on the MSDS
- Do not switch on lights or other electrical equipment, as any spark could detonate combustible gas that may be present.
- If a Hazardous Materials Response Team has been dispatched to conduct the cleanup, do not re-enter the area until it is completely decontaminated and the all-clear has been given by the Hazardous Materials Response Team or other authorized persons.

6.4.6 Menacing Person/Weapons Threat

Emergency Actions - If there is a potentially dangerous person that appears to be menacing or threatening to you or others in the general area, you should:

1. **Call 911** when it is safe to do so.
2. Notify other personnel and adjoining offices of the impending danger.
3. If you are in a position to explain your situation, give as much information as possible to the 911 operator, to include your location: department, building, office/area, etc.
4. If personally approached, stay calm and cooperate with the person. Do not make any sudden movements.
5. When safe to do so, quietly leave the area if at all possible.

6.4.7 Harassing/Obscene Telephone Calls

If you are receiving harassing or obscene calls, the best way to handle the situation is to immediately hang up without saying anything to the caller. If the caller does not receive a response, he/she will usually stop calling.

If the calls are threatening in any way, or are continuous, please contact the telephone company for additional information. They can assist in tracing the caller and notifying the Police. Have the following information available;

- Your name, address/location, phone number, and extension number if applicable.
- Date and time of harassing calls.
- Content of the calls.

If any harassing or obscene messages are left in your voice mail box, save those messages in case they are needed for evidence and notify your supervisor.

In most areas, harassment and placing any harassing or obscene telephone calls is a crime under both state and federal laws. These laws have penalties of imprisonment and/or fines. You should notify your supervisor of any repeated harassing or obscene calls.

6.4.8 Kidnapping/Hostage Situation

Emergency Actions - For any situation involving either a kidnapping or a person being held hostage, you should:

- Immediately **Call 911**.
- Remain calm and cooperate with the person.
- Make no sudden movements.
- If safe to do so, alert other personnel that an emergency/danger is present or imminent and quietly leave the area.
- Notify your supervisor or appropriate individual at your Command.

If you receive a telephone call regarding a kidnapping/hostage situation, you should:

- Keep the caller on the line to get as much information as possible.
- Use the **KIDNAPPING/HOSTAGE SITUATION CHECKLIST** located at Attachment B 8 to record all information.
- Call 911 or the local police to report the incident and provide all pertinent information
- Notify your supervisor or appropriate individual at your Command.
- **If you receive a ransom note, call 911 at once.** Minimize additional handling of the note until it can be delivered to the proper authorities. Also notify your supervisor or appropriate individual at your Command.