



*Federal Protective Service*

# Security Guard Information Manual

Secure Facilities, Safe Occupants

**For Official Use Only**



**U.S. Immigration  
and Customs  
Enforcement**

Inside Front Cover  
Left Blank Intentionally

# Contents

<b>Chapter 1: The Department of Homeland Security and the Federal Protective Service</b> .....	1
1.1: Overview of the Department of Homeland Security (DHS) .....	1
1.2: Overview of Immigration and Customs Enforcement (ICE) .....	1
1.3: Overview of the Federal Protective Service (FPS) .....	1
1.4: Five Types of Facilities and Security Levels .....	3
<b>Chapter 2: The Security Guard</b> .....	5
2.1: Your Roles and Responsibilities .....	5
2.2: Typical Duties .....	6
2.3: Creating a Good Image .....	8
2.4: Basic Appearance Standards .....	9
2.5: Acceptable and Unacceptable Conduct .....	11
2.6: Interacting with People .....	13
2.7: Sexual Harassment .....	15
2.8: Traits of a Top-Notch Security Guard .....	16
<b>Chapter 3: Federal Laws and Regulations, Crimes and Procedures</b> .....	19
3.1: Understanding Federal Laws and Regulations .....	19
3.2: Common Offenses .....	20
3.3: Reporting Incidents to the FPS MegaCenter .....	23
3.4: Jurisdiction .....	24
3.5: Search and Seizure .....	25
3.6: Detainment Authority .....	25
3.7: The Use of Force .....	26
3.8: Crime Scene Protection and Evidence Procedures .....	26
3.9: Testimony .....	27
<b>Chapter 4: Security Guard Contract Administration</b> .....	29
4.1: Your Job as a Security Guard .....	29
4.2: Relationship Between the Contractor and the Government .....	29
4.3: The Post Duty Book .....	30
4.4: Work Schedules .....	30
4.5: Weapons and Equipment .....	30
4.6: Posts .....	33
4.7: General Response Procedures .....	34
4.8: Emergency Plans .....	34
<b>Chapter 5: Controlling Access and Egress</b> .....	37
5.1: Why Control Access and Egress .....	37
5.2: Personnel Control .....	37
5.3: Property Control .....	38
5.4: Vehicle Control .....	39
5.5: Lock and Key Control .....	39

<b>Chapter 6: Intrusion Detection, Assessment and Response</b> .....	41
6.1: Means of Detecting Intrusions .....	41
6.2: Assessing Possible Intrusions .....	42
6.3: Intrusion Response Procedures .....	42
<b>Chapter 7: Facility Safety Procedures and Response</b> .....	45
7.1: The Basics of Facility Safety .....	45
7.2: Fire Alarm Systems .....	45
7.3: Response Procedures .....	46
7.4: Knowledge and Use of Fire Extinguishers .....	46
7.5: Acts of God or Other Serious Situations .....	46
<b>Chapter 8: Records and Reports</b> .....	47
8.1: Signing In and Out .....	47
8.2: General Guidelines for Report Writing .....	48
8.3: Collecting Information for Reports .....	48
8.4: Taking Notes .....	49
8.5: Report Writing .....	50
8.6: Filing Reports .....	50
<b>Chapter 9: Special Situations</b> .....	51
9.1: Escort Duties .....	51
9.2: Dealing with Seriously Disruptive Behavior .....	51
9.3: Code Adam .....	52
<b>Chapter 10: Emergency First Aid</b> .....	53
10.1: First Aid/CPR/AED .....	53
10.2: Blood Borne Pathogens .....	53
<b>Chapter 11: Combating Terrorism</b> .....	55
11.1: What is Terrorism and Who Are Terrorists .....	55
11.2: Types of Terrorists Attacks .....	56
11.3: Weapons of Mass Destruction (WMD) .....	56
11.4: Preventing Terrorist Attacks .....	56
11.5: Responding to a Terrorist Attack .....	57
<b>Chapter 12: Workplace Violence</b> .....	59
12.1: What is Workplace Violence .....	59
12.2: Who Commits Violent Acts and Why .....	59
12.3: Preventing Workplace Violence .....	60
12.4: Responding to Incidents of Workplace Violence .....	60
<b>Chapter 13: Civil Disturbances</b> .....	61
13.1: Types of Civil Disturbances .....	61
13.2: Impact of Civil Disturbances .....	61
13.3: Demonstrations .....	62
13.4: Response Procedures .....	62

<b>Chapter 14 Bomb/Weapons of Mass Destruction, Threats and Incidents</b> .....	63
14.1: Receiving Bomb/WMD Threats .....	63
14.2: Reporting Bomb/WMD Threats .....	64
14.3: Locating and Handling Suspicious Items .....	64
14.4: Response Procedures .....	65
<b>Chapter 15 Hostage Situations</b> .....	67
15.1: What is a Hostage Situation .....	67
15.2: Reacting to Hostage Situations .....	67
<b>Chapter 16 Sabotage and Espionage</b> .....	69
16.1: What are Sabotage and Espionage? .....	69
16.2: Deterrence, Prevention, and Response to Incidents .....	69
<b>Chapter 17 Child Care Centers</b> .....	71
17.1: Child Care Centers in Federal Buildings .....	71
17.2: Your Responsibilities .....	71
<b>Appendix 1: Regulations Affecting Federal Property</b> .....	73
Title 41—Public Contracts and Property Management; Chapter 102—Federal Management Regulation; Part 102-74 Facility Management; Subpart C—Conduct on Federal Property .....	73
U.S. Code, Title 18—Crimes And Criminal Procedure; Part I—Crimes; Chapter 44—Firearms .....	76
<b>Appendix 2: Sample Forms and Reports</b> .....	77
Bomb Threat Questionnaire .....	77
Questions derived from FBI Bomb Data Program Card .....	79
<b>Appendix 3: Practice Written Examination and Answer Key</b> .....	81
Information, Guidelines and Helpful Hints for Taking the Written Examination .....	81
Practice Examination .....	82
<b>Appendix 4: FLETC Use of Force Model (Form SH-8704, Rev. 04/99)</b> .....	85
Introduction .....	85
Use of Force Model .....	85
Officer Perception .....	85
Subject Action .....	86
Officer Response .....	87
Color Correlation .....	87
Tools, Tactics and Timing .....	88

Page iv  
Left Blank Intentionally

# Chapter 1

## The Department of Homeland Security and the Federal Protective Service



This section provides an overview of the mission of DHS, ICE and FPS. It will also describe the different types of work places that you may be protecting. In order for you to appreciate the importance of your job, you need to understand the mission of DHS, the role that FPS plays and the different environments in which you may be working.

### 1.1: Overview of the Department of Homeland Security

The National Strategy for Homeland Security and the Homeland Security Act of 2002 served to mobilize and organize our nation to secure the homeland from terrorist attacks. This exceedingly complex mission requires a focused effort from our entire society if we are to be successful. To this end, one primary reason for the establishment of DHS was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation. In order to better do this and to provide guidance to the 180,000 DHS men and women who work every day on this important task, the department developed its own high-level strategic plan. The vision and mission statements, strategic goals and objectives provide the framework guiding the actions that make up the daily operations of the department.

#### Vision

Preserving our freedoms, protecting America... we secure our homeland.

#### Mission

We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against as well as respond to threats and hazards to the nation.

We will ensure safe and secure borders, welcome lawful immigrants and visitors and promote the free-flow of commerce.

### 1.2: Overview of the Immigration and Customs Enforcement

With the establishment of DHS, the functions, expertise, resources and jurisdictions of several once-fragmented border and security agencies were merged and reconstituted into ICE, DHS's largest investigative bureau. The agencies that were either moved entirely or merged in part, based upon law enforcement functions, included the investigative and intelligence resources of the United States Customs Service, the Immigration and Naturalization Service and FPS.

### 1.3: Overview of the Federal Protective Service

FPS is responsible for delivering a comprehensive physical security and law enforcement program in all GSA owned or leased facilities. This involves providing law enforcement and security for more than a million federal workers and visitors at over 8,300 buildings nationwide. FPS enforces laws and regulations governing public buildings, maintains law and order and protects life and property in federally controlled work places.

At FPS, our goal is to become a premier facility security organization that provides a safe environment in which federal agencies can conduct their business. To accomplish this, we will reduce threats posed against federal facilities. These threats range from the most catastrophic, but least probable

(terrorist attacks), to the most probable but least catastrophic (larcenies), with work place violence falling at the center of this continuum.

FPS is committed to ensuring the appropriate level of security is in place at each federally controlled facility throughout the country, regardless of its location. FPS is ready to respond to our customers' security and law enforcement needs.

FPS partners with other federal, state and local agencies throughout the nation to develop specific solutions to challenges; assists with police emergency and special security services; and offers police and security support to law enforcement departments during high-profile and sensitive events. To make federal facilities safer, FPS also consults with building owners and tenants to advise them on physical security measures. FPS provides crime prevention education for agencies and individuals, and recommends strategies to keep everyone safer, both on and off the job. Services fall into eight components: Administrative Support, Communications, Criminal Investigations, Law Enforcement, Management, Physical Security, Security Guard Services and Security Systems. The organization is comprised of the headquarters and eleven (11) regions.

### **Administrative Support**

FPS's administrative support team performs all other functions not described above, such as contracting, budgeting, quality assurance, suitability adjudications and clerical support. You may encounter some of these personnel, although most of your contact will be with FPS law enforcement personnel.

### **Communications**

Four (4) FPS MegaCenters provide communications for security and law enforcement activities on an inter-and intra-regional basis. The centers also act as information and control hubs during emergency situations. Open 24 hours a day, 7 days a week, the MegaCenters monitor alarms, receive customer calls, dispatch law enforcement and emergency personnel, and retrieve information from other government agencies. As a security guard, you will have frequent contact with the FPS MegaCenter.

### **Criminal Investigations**

FPS Special Agents (SA) are non-uniformed agents who investigate crimes that occur on federally controlled property. Investigators interview suspects and witnesses, conduct searches and seizures and collect and present evidence. These agents carry firearms and enforce federal laws for the protection of people and property in federal facilities.

### **Law Enforcement**

The FPS law enforcement personnel are the most visible component of FPS's law enforcement operations. They respond to and investigate reports of crime, provide advice to client agencies on security issues, work with client agencies to improve facility and social conditions, and protect client agency operations and lawful assemblies from unwarranted disruptions.

### **Management**

FPS's management, both at the headquarters and at the regional level, is responsible for developing and providing programs, policies, leadership, guidance and oversight for FPS personnel.

### **Physical Security**

FPS physical security specialists (PSS) and inspectors conduct security assessments of federally controlled buildings and advise client agencies and employees about pertinent physical security issues affecting them. Security assessments identify the security needs of individual facilities and recommend the most effective security measures to protect the facilities. PSSs conduct recurring on-site inspections that objectively evaluate criteria such as the environment, crime rate, physical structure, tenant mix and architectural features to create a comprehensive assessment.

Additionally, PSSs usually recommend the position and hours of operation of the guard posts in federally controlled facilities and develop post orders for each post in coordination with tenant agencies and other key personnel. The implementation of security countermeasures, to include contract guards, are approved and paid for by the tenant agencies.



## Security Guard Services

FPS relies on security guards such as you to protect federally controlled property throughout the nation. You are the most visible security presence and the first public contact with security upon entering the facility. Although you are not employed by the federal government, you have a crucial role in FPS's mission and operations. We value the support provided by you to assist the FPS security team.

Your primary responsibilities are to control access to federal property; to assist in ensuring the safety of employees and visitors while on federal property; and to assist in ensuring the safety of federal property. Access control includes checking visitor and employee identification; operating security equipment such as x-ray machines and Magnetometers to screen for prohibited materials; operating or monitoring security cameras and/or alarms; and reporting crimes and incidents to the FPS MegaCenter.

FPS relies heavily on you to be the “eyes and ears” while accomplishing your security mission. You should always be aware of your surroundings and the people with whom you interact. If you notice something out of ordinary that is suspicious, you should document it and report it to the FPS MegaCenter and your supervisor in accordance with your post orders. If a crime or serious incident occurs in your facility, you will be one of the first people interviewed to see what information you can supply to assist in the investigation.

## Security Systems

Electronic security system specialists design, install, maintain, repair and operate security systems for federally controlled facilities. This group also develops cost estimates, prepares contract specifications and monitors contractors' performance on FPS contracts for security system installations. As a security guard, you may come into contact with these individuals when they are installing or repairing security equipment at your post or in your assigned facility.

## 1.4: Five Types of Facilities and Security Levels

The list below was developed by a federal inter-agency working group (including FPS), headed by the U.S. Department of Justice. The facility types were published in the Department of Justice Vulnerability Assessment of Federal Buildings, dated June 28, 1995. You should know the profile, characteristics and tenants of the facility you are assigned to.

### Level I

Typically, the Level I facility houses 10 or fewer federal employees in a space not greater than 2,500 square feet. There is a low volume of public contact or contact with a small segment of the population. A military recruiting office is an example of a small Level I “store front” type facility.

Some characteristics of a Level I facility are:

- the federal organization is a single tenant in a leased office;
- the building has no set back from the surrounding streets;
- there are other offices or businesses in the building;
- there is meter or public parking immediately adjacent to the building;
- the standard hours of operation are less than 12 hours per day;
- it does not have perimeter lights;
- it may have a simple power back-up feature for emergency lighting and fire detection systems;
- the facility most likely has high-security locks on all exterior doors; the locks are probably the only measure of security for this level facility; and
- security guards are not typically assigned to a Level I facility.

## Level II

Typically, the Level II facility has between 11 and 150 federal employees with a moderate volume of public contact. The federal activities are routine in nature, similar to commercial activities. The buildings are from 2,500 square feet to 80,000 square feet. A typical Level II building is a Social Security Administration office.

Some characteristics of a Level II facility are:

- the building most likely is a multi-story structure;
- the building probably is older. There are many historical buildings in this category;
- except for a sidewalk, the building may have no set back from the surrounding streets;
- only exterior parking is available and it is adjacent to the building; and
- the building operates an average of 12 hours per day.

## Level III

Typically, the Level III facility has between 151 and 450 federal employees. In addition, the facility probably has between 80,000 and 150,000 square feet of space and a moderate to high volume of public contact. The tenant agencies may include law enforcement agencies, court-related agencies and functions, and government records and archives. The Pension Building, a multi-tenant, historical building in Washington, D.C. is an example of a typical Level III building.

Some characteristics of a Level III facility are:

- although the building has a greater set-back than would be found at a lower level facility, it still has only a minimal setback from the street;
- it is likely to have an exterior parking lot;
- the building is open for use and operation to employees more than 12 hours per day;
- as in the lower levels, the primary security in the building is locks on all perimeter doors;
- it also may have a centrally monitored intrusion detection system; and
- the building was constructed less than 25 years ago.

## Level IV

Typically, the Level IV facility has 451 or more federal employees housed in more than 150,000 square feet. The facility usually has a high volume of public contact. The tenant agencies may include high-risk law enforcement agencies, courts, judicial offices and offices housing highly sensitive government records. For example, a typical Level IV building is the Department of Justice Headquarters building in Washington, D.C.

Some characteristics of a Level IV facility are:

- it may be set back from the street;
- it will have some interior underground parking as well as exterior parking;
- the building is accessed by employees more than 12 hours per day and may be open to employees 24 hours per day;
- public access is limited to less than 12 hours per day.

## Level V

The Pentagon and CIA Headquarters are examples of Level V facilities. Level V facilities contain mission functions critical to national security. The missions of Level V facilities require that tenant agencies secure the site according to their own requirements. The degree to which these requirements dictate security features in excess of those for a Level IV is established by the individual agency. A Level V facility will be similar to a Level IV facility in terms of number of employees and square footage. Security requirements at Level V facilities should be at least the same as at a Level IV facility.

# Chapter 2

## The Security Guard



This chapter will provide the necessary elements for you to understand exactly what is expected and required of you. It will explain for you your mission, the desired qualities for a FPS security guard, and the proper protocol when conducting business with employees of the building and visitors to the facility.

### 2.1: Your Roles and Responsibilities

Recent events demonstrate the need for FPS to focus on and increase security within our federally controlled facilities. You are an important part of the security program designed to protect these facilities. You will protect not only these facilities but also the many people who work in and visit these buildings every day. You will help the FPS enforce rules and regulations and maintain law and order. The federal government has established a contract with your employer to provide security guard services to support FPS. How you will accomplish these tasks is established by the contract and post orders. It is very important for you to understand your job because everything that you do on duty will ultimately affect the accomplishment of the FPS mission.

Most people visiting a federal building do not know you work for a contractor. To these people, you represent FPS. If you do not perform your duties at the expected standard, the consequences could be damage to or loss of federal property, serious injury to personnel or even loss of life.

Your role is to support the FPS mission. Although FPS law enforcement personnel are sworn law enforcement officers, security guards are not. You must understand the distinction between local or state police, FPS law enforcement personnel and yourselves as security guards.

Local or state police are responsible for keeping public order, enforcing laws, preventing crime and apprehending criminals. They work mostly on public property, but they may enter private property when invited or called to restore order and enforce the law. However, searches, arrests and other activities on private property are strictly controlled by constitutional limitations and laws; an example is the requirement for arrest or search warrants based on probable cause. Local or state police also may patrol private property to which the public has free entry, such as shopping center parking lots.

FPS law enforcement personnel can make arrests on and off federally controlled property. Special agents (SA's) investigate crimes ranging from homicide to theft of government property. They also investigate allegations of security guard misconduct on the job. Information you provide to FPS investigators can be important to the successful outcome of a criminal investigation. FPS uniformed and investigative personnel or local law enforcement (depending on your post location) will serve as your primary law enforcement support as you perform your duties.

Security guards help keep public order and prevent crime. You can detain individuals who are being seriously disruptive, violent or suspected of committing a crime while on federally controlled property, but you do not have the authority to arrest a suspect as police. Your duties mainly concern preventing and detecting crime rather than investigating and solving crimes. As part of your assigned duties you are expected to:

- control access to specific areas of a facility;
- enforce property rules and regulations;
- detect and report criminal acts;

- stop and if possible, detain persons engaging in criminal activities;
- provide security against loss from fire or mechanical equipment failure;
- respond to emergency situations involving the safety and security of the facility; and
- act occasionally as a crowd monitor to maintain order.

These duties will be discussed in much greater detail in the chapters that follow.

## 2.2: Typical Duties

As a security guard, you will have many duties. Typical duties are described below and several will be explained in further detail later in this manual. Your specific duties will be detailed by post orders or by the contracting office technical representative (COTR) in event of an emergency. During your career as an FPS security guard, you may be required to perform most or all of the duties described below.

### Access and Egress Control Post

You must be mentally alert and physically ready to operate and enforce the government's system of personnel identification and access/egress control as it is stated in your post orders. You may need to perform inspections, either as part of your regular duties or during periods of heightened security alerts. These inspections may include checking packages, briefcases, containers or any other suspicious items in the possession of people entering or leaving a federally controlled facility. Your inspections will normally focus on ensuring visitors do not bring weapons, bombs/bomb-making materials, chemical/biological agents or other prohibited materials into the building. You will also focus on ensuring persons do not depart the building with government material unless they are in possession of a valid property pass, if applicable.

You may be responsible for operating security equipment on your assigned post, such as x-ray machines, magnetometers and intrusion detection and closed circuit television (CCTV) systems. You will receive training on the use of the equipment.

You will deny and prevent entry to those persons refusing to submit to a voluntary inspection, except for those persons exempted by a specific government directive, which will be included in the post orders.

You will provide on-site security and control access to the post area by detecting, observing and reporting violations of post regulations. This includes security of all internal and perimeter areas designated within the confines of your assigned post.

You will answer general questions and provide directions to visitors and building tenants. You must be familiar with each tenant agency's name and the locations of the most commonly sought after offices, elevators, entrance/exit points, convenience areas (restrooms, cafeteria, etc.), within the facility.

You must know the location of and have the ability to use any/all emergency equipment associated to your assigned post area. This includes the first aid kit, automatic external defibrillator (AED), fire extinguisher, fire alarms or duress alarms. Your post orders will provide direction on implementation.

### Additional Duties

Dependent upon location, additional duties may encompass turning off unnecessary lights, checking safes/lock-type repositories and cabinets, closing and securing open windows/doors/gates or other access points, raising and lowering the flag or other duties directed by post orders.

### Building Rules and Regulations

You will observe and monitor building occupants and visitors for compliance with the facility's posted rules and regulations. You shall also identify, report, delay or detain those persons who violate the rules and regulations as applicable and in accordance with the post orders.

### Civil Disturbances

You may be required to take actions to control crowds during civil disturbances. You also may be required to assist law enforcement personnel during such situations as directed by the COTR.

## Control, Issuance and Storage of Keys

Based on your post orders or direction from your COTR, you may be required to coordinate the receipt, issuance and tracking of all keys, key cards, lock combinations, etc. which control/restrict access to the facility. Access to these aforementioned items as well as issuance and tracking procedures will be in accordance with guidance contained in your post orders. Removal of any of these items from the facility/property is strictly prohibited unless authorized by the COTR or the post orders.

You will immediately report any missing, lost, stolen or unusable key(s) or access control device to the FPS MegaCenter, COTR and shift supervisor.

As a security guard, control of the keys and access devices for the facility is a serious responsibility. Any negligence on your part resulting in these items being lost, damaged or used by unauthorized individuals would result in an investigation and your employer determining if any/or what disciplinary action is warranted.

## Emergencies

Emergency conditions require immediate attention and action and you may be required to respond. Depending on the nature of the emergency, you may have to contact the appropriate personnel as outlined in the building's Occupant Emergency Plan, which should be incorporated into your post orders. Emergency conditions may require you to be diverted from your normal duties until the emergency is over.

## Hazardous Conditions

You shall report and record all potentially hazardous conditions and items in need of repair, including inoperative lights, leaky faucets, toilet stoppages and broken or slippery floor surfaces.

## Physical Security and Law and Order

You shall maintain physical security and law and order within your area of assignment as prescribed by statute, regulation or post orders. You may be responsible for detecting, delaying and/or detaining persons violating laws, rules and regulations.

## Primary Security Response

If your work site is in an outlying area, or in the event of multiple incidents, you may be required to be the primary security responder until law enforcement personnel arrive. This will require you to be familiar with your post orders, to remember your training and to apply yourself as the situation may warrant.

## Reports, Records and Testimony

You will prepare required reports regarding security-related incidents/occurrences such as accidents, fires, bomb threats, unlawful acts, etc., and provide these reports to those officials specified by your supervisor and/or COTR.

You shall verbally report threatening circumstances/potential threatening activities that you observe while on duty to the FPS MegaCenter and your supervisor. Whenever possible, you should report a serious/potential serious problem before responding so you may receive additional guard backup and/or whatever other support is necessary to lessen or eliminate the problem.

You may be required to testify in various judicial proceedings on behalf of the Government. Your employer will coordinate all contract-related court appearances with the COTR when such appearances are required. You will be paid for all time associated with court duty, whether or not your testimony is provided or used in the case. Contract-related court testimony on behalf of the Government shall take priority over all your other scheduled duties. Unless otherwise required by the COTR, you shall appear for court testimony wearing your full uniform without any firearm or weapon.

## Response to Injury or Illness

You shall obtain professional assistance in the event of injury or illness of individuals while they are in the facility. You may be required to perform first aid, CPR and/or use the AED equipment in emergency situations and properly assist medical and law enforcement personnel as necessary and when trained or certified to do so.

## Roving Patrols

You will conduct patrols in accordance with routes and schedules contained in your post orders. You will observe, report and respond to all suspected or actual security violations or facility problems. You will be responsible for initiating and maintaining all necessary documents, reports or files for any incidents/occurrences while performing your assigned duties. Your security patrol duties and associated functions will be performed in a professional manner at all times, observing the area and questioning any person(s) whose activities do not appear normal. As the rover, you will usually be required to respond to any alarms, calls for assistance or emergency situations.

## Security and Fire Systems

You may be required to monitor and operate building fire alarm and intrusion detection systems and other protection devices or building equipment located on or near your post.

## Traffic Control

Depending upon your location and based on your post orders, you may be required to direct traffic (vehicular and/or pedestrian), control parking, issue courtesy traffic violation notices on federal property, as well as observe the environment for suspicious vehicles or persons on or around federal property. You may be required to operate traffic control points and identify, delay and detain any suspicious vehicles or persons as required to maintain the appropriate level of security to ensure the safety and protection of all personnel, property and resources within the facility.

## Unauthorized Access

You shall prevent, discover, delay and/or detain persons attempting to gain unauthorized access to property and/or personnel at the facility being protected. You shall report all such incidents in accordance with established procedures detailed in the post orders.

## Utility Systems

You may be required to lock or unlock specific access and egress points, and turn on/off lights in your duty area at specific times during your tour of duty.

During emergencies, you may be required to perform simple emergency related functions that activate or deactivate building systems, such as heating/ventilation/air conditioning systems, circuit breakers/switches and plumbing valves/switches.

## 2.3: Creating A Good Image

First impressions of a guard in uniform “says a lot” for some people, whether employees in the building or visitors. A sharp appearance and courtesy will enhance your relations with people. Your professionalism in dealing with the public helps build a good image for your employer and instills a sense of trust in the client agency you protect. While you are on duty you represent FPS, the government and your employer. You will usually be the first person a visitor meets upon entering a federal facility and therefore, you have an obligation to always make a good impression.

Being an FPS security guard requires high standards and the appropriate use of discretion. In your position you may have access to information that is either proprietary or on a need-to-know basis. You may be approached by people who ask you questions of a sensitive nature (e.g., about building security, government policies, active investigations, etc.). Your response to these questions are crucial. If you divulge sensitive information, you could be subject to disciplinary action, up to and including the permanent removal from all FPS security guard service contracts and possibly criminal prosecution. Someone asking questions of a sensitive nature concerning the federal government or employees of the same should always be referred to the government agency for answers.

Your discretion applies to matters of both an official and non-official nature. The possibility exists that someone could overhear your conversation and take it out of context. Comments about a sensitive matter may be reported to your superiors and if investigated and found to be true, you may be subject to disciplinary action. Always be mindful of your conversations and those personnel around you.

As a FPS security guard, you should be aware of the fact that any type of unprofessional behavior will not be tolerated and could result in you being removed from an assigned post or from the contract.

Building trust and goodwill are two of your many important functions. Cultivate good relations with employees at your workplace. Their safety is one of your responsibilities. This may be accomplished by a courteous greeting (e.g., good morning, good afternoon), by addressing them by name whenever possible (e.g., Mr. Smith, Ms. Jones). If their names are unknown a polite “sir” or “ma’am” would be appropriate.

When making a request of someone, saying “please” before and a “thank you” after goes a long way (for example, “Sir, could I please see your identification?” and “thank you” after they comply). Gestures such as these not only make you appear to be professional and courteous, but also provides the people you are addressing a feeling of respect.

Many buildings have VIPs working within or who regularly visit the facility, such as executive management, elected officials and judges. If your duty book contains a VIP listing with names and pictures, you should make every effort to memorize them so you can greet the VIPs by name. By doing so you are creating a positive impression that reflects your professionalism once again. There have been many instances when a VIP has taken the time to write a letter of commendation on behalf of a security guard who has shown continued professionalism and attention to duty. It is well worth the small effort it takes to act professionally and courteously at all times.

## Professionalism

**Professionalism for a FPS security guard is a cornerstone for your foundation.** Your attitude and actions should clearly show everyone your intent to perform your duties to the best of your abilities and they in turn should cooperate and allow you to do so. You must exercise caution and be mindful when balancing friendliness and politeness with firmness. You are there to provide protection. Even in the face of people being rude or abusive towards you, your demeanor should remain professional and courteous. It’s essential to be friendly, but never to the point where people will expect you to bend or break the rules. You will come to know and recognize employees within the facility and it would be simple to “allow one to enter who has forgotten his/her identification one day, for example.” In an

instance such as this, and although this may be one of the nicest persons you have met, you must follow your prescribed duty and process this individual as outlined in your post orders. Never place yourself in a compromising position.

## 2.4: Basic Appearance Standards

The following are basic standards for all security guards. Since you are a representative of your company, FPS and the government, you must meet the highest standards for appearance. Your appearance is a subtle, silent form of communication.

### Personal Appearance

You are expected to be clean and properly groomed at all times. Your uniform must be clean and unwrinkled when you report for duty.

Your fingernails should be free of dirt and trimmed so that they do not extend beyond the fingertips. Nail polish may be worn if it is subdued and natural looking.

Your hair must be clean, neat and not interfere with the proper wearing of official headgear. The height of the hair (male or female), from the scalp to the highest point on the coiffure, is not to exceed 2 inches. Hair must not fall below either the eyebrow when the head is uncovered nor protrude below the inside sweatband of headgear. A male security guard’s hair must not cover the top of his collar when standing. A female security guard’s hair cannot exceed below the bottom edge of her blouse collar when standing. Bouffant and modified bush styles are acceptable if they allow proper wearing of the official headgear.

Hair ornaments, such as flowers and combs, cannot be worn. Items to hold hair in place such as bobby pins, hairpins and barrettes may be worn if they are concealed as much as possible and are of a color that blends with the hair. The cap may be secured to the hair with up to two hatpins of plain design with black or dark blue pinheads.

Faces must be clean-shaven, except for mustaches and sideburns. Men’s sideburns must be neatly trimmed, extending no lower than the bottom of the ear, constant in width (not flared), and end with a clean-shaven horizontal line.

Mustaches are to be neatly trimmed, they may extend no more than a half-inch beyond and a fourth-inch below each corner of the lips and go no higher than the nose line.

Upon submission of a medical certificate from a licensed physician stating that a skin disorder exist and the individual cannot shave, he may wear a beard provided the beard hairs are trimmed symmetrically and do not protrude more than one-fourth of an inch from the skin's surface. The permission to be unshaven is granted only for the duration of the skin disorder. Therefore, the physician's certificate must be updated every 120 days, unless the physician's initial certificate stipulates the disorder may exceed beyond 120 days.

Makeup may be worn by security guards, provided it is subdued and natural looking.

While you are on duty, you may not wear jewelry such as earrings, bracelets, chains, religious insignia, buttons or pendants. You may wear a ring, but only on the third finger of one hand. You may wear a necklace, but only if it is completely concealed beneath the uniform shirt. You must remove ALL body piercing jewelry prior to working on post unless it is completely covered by your uniform. These rules may seem restrictive to you, but they are for your own protection. Violent offenders have been known to rip earrings out of ears and make garrotes with necklaces.

Undergarments that can be seen through or above a uniform shirt must be white. Female security guards must wear supportive brassieres.

### **Proper Wear of Uniforms**

Keep your uniforms, insignia, accessories and equipment clean and in good repair. They are to be maintained and worn as follows:

Wear your cap squarely on the head, with the sweatband snugly against the forehead, except when you are in a motor vehicle or assigned to an office. However, the cap must be in your possession at all times while on duty. You may be issued a dark blue fur or pile-trimmed cap with earflaps in cold weather.

Long-sleeved shirts may be worn as under or outer garments; however undergarments shall not be seen under the natural line of the uniform. Short-sleeved

shirts may be worn as outer garments or under the windbreaker. When you wear a long-sleeved shirt you must wear a tie. When the shirt is used as an outer garment, do not wear suspenders, do not roll/fold back the sleeves. You may have a shirt altered only for proper fitting.

Leave trouser legs un-cuffed and hem at the point where they touch the shoe tops without breaking the creased lines. Trousers must fit properly.

Wear a solid black, 2- or 3-inch-wide, clip-on tie with long-sleeved shirts. Use an appropriate law enforcement or plain tie clasp or pin. Do not tuck the tie into the front of the shirt. Do not wear a tie with a short-sleeve shirt.

An overcoat or windbreaker may be issued to guards assigned outside duties in cold weather. Any outerwear worn must first be approved by FPS. All outerwear must display your nameplate and badge.

Wear black socks that are long enough so that your skin won't show below your trousers when you are sitting. You may wear white socks if they are required for medical reasons and you are authorized to do so.

Keep your footwear shined and in good condition. Shoes must be black with black laces and plain toes. Toes and heels are to be closed and the heels no higher than 1 (one) inch. Pumps, loafers, wingtips, sandals, suede and athletic shoes are not permitted. If boots are worn, they must be black with rounded plain toes (not pointed). Boots with decorative stitching, heels higher than 1 inch or tops higher than 12 inches are prohibited. Do not tuck trouser legs into the tops of boots.

All badges must be of a type approved by or issued by the contractor. Wear the metal breast badge on the left breast of the shirt when the shirt is used as the outermost garment. Wear the cloth badge on the windbreaker and overcoat. Wear the cap badge squarely upright and centered above the cap visor.

Shoulder patches must conform to the contract. Wear the contract security guard service patch on the left shoulder of the shirt, overcoat and windbreaker.

The nameplate is metal with round corners and measures 2½" long, 5/8" high, with letters ¼" high. The nameplate contains the guard's first initial and



last name. Wear it centered on the right pocket flap of your outermost garment. Nameplates must be of the same material and appearance for all security guards.

Wear only the accessories that you are qualified to handle and are issued by your employer in accordance with the contract. These include but are not limited to: handcuff case with handcuffs, key holders (which may be worn on the trouser belt), radio case and baton. For security guards working on armed posts, equipment includes an FPS approved holster worn at the hip, a sidearm, an ammunition pouch with ammunition and four pistol belt keepers.

**You are prohibited from carrying or using the following; personal weapons, the klieg-light flashlight, knives, blackjacks, rifles or any other items not specified by the contract.**

Uniforms and equipment must be worn or in your immediate possession at all times.

### Care of Uniforms and Equipment

You and your employer are responsible for maintaining and controlling all approved uniforms and equipment. Agencies may, at some locations, provide office and locker facilities.

Weapons, nightsticks or batons, handcuffs, flashlights, hand-carried communication devices (e.g., radios or cell phones) and building keys will be controlled according to post orders and logged in on DHS Form (TBD), Firearms and Equipment Control Register. Unless otherwise authorized by the contract/post orders, weapons will be stored in a government approved steel safe or approved locker when not in use. Record the weapon's serial number and the number of bullets on the DHS Form (TBD). (Note: Some FPS contracts require or authorize security guards to take their weapons off the post, and in such cases no on-site safe or firearms cabinet will be available for weapons storage. Your post orders will describe the procedures for transporting and/or storing weapons under these circumstances).

If you remove any equipment from the building or facility, indicate so on the same form and note in the building log the date, location and reason for removing the property.

You must be prepared to make all equipment listed on the DHS Form (TBD) available for inspection by FPS personnel. The inspectors are required to identify themselves with FPS credentials. The building log entry is to show the date, times of arrival and departure and the name of the inspector along with any remarks. If you have any questions concerning the validity of the inspection, notify your supervisor or the FPS MegaCenter. Cooperate fully with the inspector.

## 2.5: Acceptable and Unacceptable Conduct

### Acceptable Conduct

You must report for duty at the assigned time and post. It is your duty to report on time and to stay on post until you are properly relieved. You must be prepared for duty when you report. You must be in the full, proper uniform with all your required equipment to include your assigned weapon. Once you have assumed your post, you will not be allowed to take breaks unless you are properly relieved, all of which is stipulated in your post orders. Even while on break, you still are required to maintain a professional appearance. Breaks are to be taken away from the post area so it does not appear you are neglecting your duties.

### Unacceptable Conduct

Unless specifically authorized in your post orders, you are not permitted to engage in any of the following activities while in uniform and on post:

- eat, drink or use any tobacco product.
- read newspapers, books, magazines or any other prohibited reading material;
- use any type of radio, cassette player, CD player, walkman or music device;
- watch television;
- use a personal computer (e.g., laptop, PDA such as a palm pilot, etc.);
- use a personal cellular telephone;
- sleep, doze or nap;
- play cards or other games (electronic or non-electronic);
- have friends or family members on post or in the area;

- socialize with friends, building tenants, visitors or other security guards who are on break or off duty; or
- use agency offices or personnel facilities for any of the above listed prohibited activities unless on a authorized break and are permitted to use the facilities (e.g., the snack bar, cafeteria or break room...generally, any room/area open for public use).

While on duty, you cannot fraternize with the building occupants or visitors. You may engage in conversation with them if necessary in conducting official business. Because you are in uniform and are easily identified by building occupants as well as the general public, your actions could easily be misinterpreted.

You cannot use alcohol or any medication (prescription or non-prescription), which impairs your ability to perform your duties. For example, cold/allergy medicine, pain relievers, muscle relaxers, etc., all of which may affect your mental awareness. This applies to the eight hours immediately prior to assuming duty and while on duty. Using drugs or drinking on duty is grounds for immediate dismissal and removal from any federally controlled facility. FPS security guard service contracts require random illegal drug testing and illegal drug testing for reasonable cause. A positive reading on any drug test is grounds for immediate and permanent removal from every FPS security guard service contract.

As a representative of a law enforcement organization, use of illegal substances will absolutely not be tolerated, whether you engage in such activity on or off duty.

You shall not remove any property that does not belong to you, whether it is owned by employees or visitors of the facility you are protecting or the government. Any person found violating this law will be subject to disciplinary action and possibly prosecuted under Title 18 of the U.S. Code or under local laws.

Provided you have been properly relieved or your tour of duty has ended, when you leave your post you must document on all records and logs that you are not on duty. The relief security guard will sign in and work if you are on a break. A supervisor should not be providing relief because you cannot

perform both as a productive security guard and supervisor at the same time.

In the event any situation not covered in the manual should present itself, contact your supervisor for directions and/or clarification.

### Grounds for Possible Disciplinary Action

The following list with explanations comprises grounds for possible disciplinary action, up to and including permanent removal from any FPS security guard service contract.

1. Assault—making or uttering physical or verbal threats.
2. Arson.
3. Theft or pilferage.
4. Sabotage.
5. Willful or careless destruction of property or vandalism.
6. Dishonesty—accepting bribes, enabling a person to secure stolen property, permitting unauthorized access to a facility or protected materials or lying to a government official or your supervisor.
7. Misuse of weapons, whether assigned to you or not.
8. Insubordination towards the visitors, your supervisor(s) or government personnel.
9. Disregarding orders, including your post orders, special orders or instructions, or verbal instructions from your supervisor(s) or the government's contracting officer's representative.
10. Immoral conduct or any other criminal act that violates rules, regulations or established policy of the government.
11. Sexual harassment or discrimination towards visitors or government employees.
12. Intoxication—being under the influence of any substance that impairs your ability to perform your duties, such as alcohol, illegal substances or medication with impairing side effects.
13. Negligence—sleeping on duty, abandoning your post without being properly relieved or failing to perform your duties as prescribed.
14. Absenteeism—failure to report for duty or unsatisfactory attendance.

15. Tardiness—repeated failure to report for duty at the scheduled time.
16. Falsifying, concealing, removing, mutilating, damaging or destroying official documents or records or concealing important facts by leaving them out of official documents.
17. Reading, copying, removing, damaging or destroying government or proprietary business documents that you do not have access to during your normal course of duties.
18. Disorderly conduct—abusive or offensive language, quarreling, fighting or attempting to intimidate someone. This also includes interfering with normal, efficient operations or performing your assigned duties.
19. Unethical or improper use of official authority, credentials or equipment.
20. Unauthorized use of communications equipment (e.g., telephones, computers, radios) or other government property.
21. Unreasonable delays or failure to complete job assignments, conducting personal business while on duty, refusing to assist someone as required in your post orders.
22. Failing to cooperate with government officials, local law enforcement officials or your employer during an official investigation.

## 2.6: Interacting with People

Success in security and law enforcement depends largely on the ability to interact with people from all walks of life effectively. People react to how you look, how you act, how you speak and how you treat them. Even though you are not a federal employee, you represent FPS as well as your employer. You are often the first contact the public has when entering a federally controlled facility and the last person they see when they leave. Visitors and employees will make immediate judgments about you based on your appearance, your demeanor, your body language and your performance. These conclusions color their impression of the agency visited and the government as a whole. The impression you make is a lasting one. People may choose to cooperate or not cooperate with you depending on how you treat them.

There are several basic guidelines for dealing with people, which are mostly common sense:

- be polite and tactful when greeting and addressing people;
- use proper English when speaking to people; speak clearly and in a well modulated tone; do not mutter or say things under your breath; never use profanity, any type of slang or disrespectful language while you are on duty;
- do not use inappropriate gestures when talking to people;
- remain calm at all times, no matter how much you are provoked; do not show anger or impatience with people; never argue with people;
- know your duties and the layout of the facility. People will often ask questions about the location of offices, people or amenities in a facility you are protecting;
- although you may feel it is not your responsibility to answer routine questions from visitors or employees, this is a very important aspect of your duties and therefore you should try to be cordial unless otherwise stated in your post orders;
- you should always maintain high standards of appearance and grooming when in uniform and on duty;
- always be attentive to your physical demeanor when on duty. Stand up straight, do not slouch, do not put your feet on desk or equipment, etc;
- be observant at all times. Be aware of people in your area and attentive to the surrounding area;
- do not rest your hand on the butt of your weapon because some people could perceive it as a threatening gesture;
- if necessary to react to control a situation, use only the minimum amount of force necessary; and
- refer any news media personnel to the FPS MegaCenter.

### Dealing with Children

In your job, you may have regular contact with children. It is very important that you understand how you should treat them and interact with them.

When dealing with children, you must try to balance friendliness with firmness. While many children

may be afraid or intimidated, others may be curious or even fascinated by you, your uniform and your equipment. You should try to make frightened children feel more comfortable by smiling and using a friendly tone when you speak to them. If they ask you what you do, tell them your job is to make sure they are safe while they are in the building.

Some children may be more outspoken, curious or even aggressive in their behavior. They may want to know about your equipment, especially your weapon(s). **Under no circumstances whatsoever should you ever unholster your firearm or display other equipment, such as your handcuffs or batons to a child.** If a child asks to see your firearm, tell him/her that you cannot take it out of the holster because it is a weapon and is only to be taken out of the holster in an emergency. **Never** allow a child to touch your equipment, even if it is secured on your belt.

Do not invite or allow a child to sit on your lap, do not pick up/hold a child, do not touch a child. Many parents/guardians become uncomfortable when adults they do not know have close contact with their children. Your attempt at being kind or helpful could result in a parent/guardian thinking your actions are inappropriate. This could lead to them filing a complaint against you and almost surely will result in an investigation being done. Try to have no physical contact with a child unless it is absolutely necessary (e.g., in an emergency situation where you are compelled to aid or quickly move a child from a dangerous threat). For any further explanation, you can contact your supervisor or refer to Chapter 17 of this Manual.

## Using the Telephone

For most people, making a call to a security guard is a very significant act. It will leave an impression as lasting as a personal encounter and may be the caller's only contact with an FPS representative.

First, the caller should be able to get through on the line. The telephone (regular or cell phone) is provided to you for communication of official business, not to initiate or receive personal calls. You are not permitted to make long-distance personal calls on government furnished telephones. (You could be

held financially liable for any charges that result from improper/unauthorized usage). People also may have a negative impression of you if they overhear you on a personal call. They could be waiting to speak with you and/or request your assistance and as such may feel you are neglecting your duties by having them wait. The improper usage of any type of government telephone could result in disciplinary action against you up to and including removal from the contract.

Secondly, the caller expects a decisive and courteous response from you. Apply the same guidelines in dealing with people when answering the telephone:

- answer in a pleasant tone and speak clearly;
- clearly state your name and location when answering;
- have a pen/pencil and notepad available to take notes; repeat the information to the caller to ensure you have copied it correctly;
- if questioned, be mindful of what you may/may not discuss over the telephone; if necessary, request a supervisor if in the immediate area.

Always handle an excited or angry caller politely but firmly. You can have a calming effect on someone by asking a caller to relax, and speak slowly so you can better understand what they are trying to tell you. If it appears the caller is confused and rambling, not making any sense, try to get them to focus on the problem by asking specific questions.

Any threats made over the telephone should always be taken seriously. Chapter 14 discusses telephone threats in more detail.

Sometimes it may be necessary to place a caller on "hold." If it is necessary to do so, advise the caller you must put them on hold prior to doing so and ensure the caller has acknowledged you. Once you return to the caller, apologize for the delay and thank them for holding. Never hang up on a person or place them on hold before prior notification.

As a final note, if it is necessary for you to take action on a call, ensure you follow-through on the issue. Failure to do so could have a negative effect on you and lead to possible disciplinary action.

## 2.7: Sexual Harassment

Sexual harassment is a serious subject. You should carefully read this section and contact your supervisor if you have any questions.

The U.S. government's Equal Employment Opportunity Commission (EEOC) has issued the following information about sexual harassment.

### Facts about Sexual Harassment

Sexual harassment is a form of sex discrimination that violates Title VII of the Civil Rights Act of 1964. Unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature constitutes sexual harassment when submission to or rejection of this conduct explicitly or implicitly affects an individual's employment, unreasonably interferes with an individual's work performance or creates an intimidating, hostile or offensive work environment.

Sexual harassment can occur in a variety of circumstances, including but not limited to the following:

- the victim as well as the harasser may be a woman or man;
- the victim does not have to be of the opposite sex;
- the harasser can be the victim's supervisor, an agent of the employer, a supervisor in another area, a co-worker or a non-employee;
- the victim does not have to be the person harassed but could be anyone affected by the offensive conduct;
- unlawful sexual harassment may occur without economic injury to or discharge of the victim; and/or
- the harasser's conduct must be unwelcome.

It is helpful for the victim to directly inform the harasser that the conduct is unwelcome and must stop. The victim should use any employer complaint mechanism or grievance system available. When investigating allegations of sexual harassment, EEOC looks at the whole record: the circumstances, such as the nature of the sexual advances and the context in which the alleged incidents occurred. A determination on the allegations is made from the facts on a case-by-case basis. (Source: EEOC)

As a security guard, you are in a unique situation because you work with government employees and the public every day but are not an employee of the U.S. government.

Your employer will have specific policies about sexual harassment, which probably include a specific complaint or grievance process you can use if you are the victim of sexual harassment by a co-worker or manager of your company. You should always follow your employer's guidance and policies on sexual harassment.

**FPS will not tolerate any act of sexual harassment by a security guard towards any other person.** Sexual harassment is grounds for immediate removal from any FPS security guard service contract. If a government employee or visitor complains to the DHS or FPS about sexual harassment by a security guard, FPS will initiate an investigation, and it is probable that the employer will be asked to make a determination about removing the individual(s) from the contract until the investigation is completed.

Keep in mind that one basis for determining whether an act of sexual harassment is if the behavior "creates an intimidating, hostile or offensive work environment" to the person being harassed. Protect yourself, your career and your co-workers/friends by following the guidance below while you are in a federally controlled facility, whether on/off duty:

- **Never** make jokes, comments or gestures of a sexual nature—even when you think you are alone and nobody can hear or see what you are saying or doing.
- **Never** touch a person in a way that can be construed as sexual in nature (e.g., hugging, touching the breast or buttocks area). Such behavior is totally unprofessional.
- **Never** engage in sexual activity while in the facility. This is completely unacceptable behavior. If discovered, it is grounds for your immediate removal from the contract.
- If you are working on a post where another security guard makes jokes or comments of a sexual nature, instruct the individual to stop immediately, and contact a supervisor immediately. While no one wants to be a "tattletale," you will place

yourself in a position for possible disciplinary action against you if you fail to say or do anything to halt the behavior, giving an appearance that you agree with or are a participant of said behavior.

- If you are working on a post and a government employee or visitor makes jokes or comments of a sexual nature, tell them that in your position you cannot participate in such discussions and that such comments make you very uncomfortable.
- Do not ask somebody out on a date or ask for information of a highly personal nature about another person (whether another security guard, government employee or visitor) while you are on duty. Wait until you are off duty and are not in the Federally-controlled building to make social engagements or get to know other people.
- Do not initiate or respond to flirtation while you are on duty. Treat everyone the same, professionally and courteously. Save the romance for when you are not in the Federally-controlled building. Even if the flirtation is welcome to the person you are flirting with, other people may be uncomfortable and could make allegations towards you because of your behavior. The appearance of impropriety is just as dangerous as the “act” itself and could affect your career.
- If you believe you are being sexually harassed by a co-worker or by a government employee, you should **immediately** contact your supervisor and inform him/her so that your company can pursue the matter with the appropriate officials. Just as you must never act in a harassing way, you should never have to tolerate sexual harassment by others.

## 2.8: Traits of a Outstanding Security Guard

The following list describes the qualities/traits that make an outstanding security guard. Not everyone has these qualities in equal measure, but they are all important. Evaluate yourself honestly and think of ways that you can improve or cultivate those qualities that are not your strengths. Because you have such important responsibilities, you must be a top caliber individual with a strong sense of duty. These are the qualities/traits that FPS considers necessary in a security guard.

### Alertness

You must be aware of the environment around you and be able to notice even the slightest changes or unusual conditions. By being observant and aware, you will prevent and detect crime or unauthorized behavior. You must watch for deviations from the norm, such as a strange car parked in an unauthorized space, a person approaching or coming from an area that is not normally used or nervousness/unstable behavior from a person approaching you. Alertness can only be achieved by keen watchfulness and by diligent application of the patrol or post requirements. Alarm systems enhance the effectiveness of security forces, but nothing is a substitute for the alertness of security force personnel. The degree of alertness determines whether security is effective or lax.

### Approachable Manner

Many people are intimidated by or fear law enforcement and/or security personnel. Try to minimize their concerns by giving signals showing that you are approachable, such as making eye contact with a smile, greeting the person cordially or simply acknowledging their presence with a nod. If you can win people’s trust, you will be able to do your job much more effectively.

### Confidence

Confidence is a state of feeling sure, free from doubt or misgivings. Confidence includes faith in oneself and in one’s abilities. Nothing can bring out self-confidence like job knowledge. You must have confidence in yourself, your equipment, your leadership and other members of the security team. If you have concerns about any aspect of your job, contact your supervisor for guidance. Generally, the more experience you have on the job dealing with a wide variety of people and situations, the more confidence you will have.

### Ethics

You must never accept gifts, benefits or favorable treatment other than authorized rewards. Similarly, you must never give preferential treatment or benefits to others, or even give the appearance of wrongdoing. Any acceptance of unauthorized or unofficial

compensation, favoritism or other benefits is unethical behavior and grounds for removal.

### **Even Temperament**

You must not get angry in performing your duties. Anger does not help in any situation. By being calm, you will prevent situations from escalating and others will become calmer.

### **Good Judgment**

Good judgment is more than the application of common sense. It is the power of arriving at a wise decision. Experience provides knowledge, and knowledge precedes judgment. Security instructions cannot cover every situation. Many are unique and require individual consideration. You must develop the ability to observe, compare and discern similarities and differences to arrive at logical conclusions. However, a word of caution—you should call the FPS MegaCenter and/or your supervisor when you are in doubt about how to proceed.

### **Impartiality**

Do not take sides in disagreements or disputes among others. You cannot show favoritism toward one side or it will be viewed as an attack against the other. You must be unbiased and simply address the facts as known.

### **Integrity**

You must be honest and above reproach. You must always do what is right, not what is simply convenient, acceptable or easy.

### **Knowledge**

To be effective, you must know your duties well. Your job is very sensitive and its guidelines are important. You must know what to do and how to do it.

### **Physical Fitness**

Security duties are often sedentary, but occasionally they require great physical exertion. You must be able to react quickly, be strong and have endurance. Emergency responses and confrontations will be very physically demanding. The security of an instal-

lation or facility may depend on your level of physical fitness and ability to act to control a situation.

### **Politeness**

You must always display courtesy and politeness when dealing with others, whether they are friendly, indifferent or hostile. You will gain respect and cooperation by being polite.

### **Positive Attitude**

Your general mental attitude towards life and your job is very important. Interest in the job and loyalty to the organizations you protect are particularly applicable to security personnel. By maintaining a positive outlook on life in general and in your job, you will be more productive, effective and satisfied.

### **Self Control**

Security duty presents situations that require not only sound judgment but also self-control. You must always act professionally and control all of your emotions, especially anger, exasperation, frustration, nervousness and fear.

### **Tactfulness**

The ability to deal with others without offending them is a highly desirable quality in security personnel. It is difficult to assume the authority and responsibilities of security duty without consciously or unconsciously displaying a sense of superiority in an overbearing manner. Security personnel must be able to communicate clearly, concisely, firmly and authoritatively but without arrogance or in an offensive manner.

Page 18  
Left Blank Intentionally



# Chapter 3

## Federal Laws and Regulations, Crimes and Procedures



Security guards must operate within strict legal and procedural guidelines; you must therefore know these guidelines in order to do your job effectively. This knowledge will help you to recognize and respond correctly to the incidents and crimes you may encounter. It will help you to avoid errors or legal difficulties when detaining suspects, writing and filing reports, and testifying in court. This chapter provides you with: a basic understanding of federal laws and regulations that pertain to your responsibilities; information on the legal authority you have as a security guard; and the proper procedures to use in executing your duties.

### 3.1: Understanding Federal Laws and Regulations

Your job as a security guard is to protect U.S. government property and the people who work in or visit federal buildings. Your authority is based on federal laws and regulations. All federal criminal laws are contained in the **U.S. Code (USC)**, particularly **Title 18—Crimes and Criminal Procedure**. Title 18 not only describes each federal crime but also contains provisions for punishment, such as fines, jail time, or both. If you have access to the Internet at home or at your employer's office, you can read Title 18 at the following Web site: [www.access.gpo.gov](http://www.access.gpo.gov). As you might imagine, Title 18 is a huge document, and it is not feasible or necessary for FPS to reproduce it in this manual. **What you need to know and remember is that virtually every crime that occurs on federal property is punishable under Title 18 USC.**

The executive branch of the federal government has developed regulations for implementing the federal laws contained in the USC. These regulations are

called the **Code of Federal Regulations (CFR)**. The federal regulations you will follow are contained in the **Federal Management Regulations (FMR)**, which is one section of the CFR. You can read these regulations through the Government Printing Offices' Web site: [www.access.gpo.gov](http://www.access.gpo.gov).

For your convenience, this manual contains the FMR sections you will use most often in your job. They are contained in Appendix 1 at the end of the manual. **Make sure you take the time to read and understand all of the regulations contained in Appendix 1, because a major part of your job is to ensure that people who enter federal property comply with them.**

### Criminal Law

A crime is an act, or failure to act, that is prohibited by public law in order to protect the public from harm. A single act could constitute crimes punishable by both state and federal laws, since separate offenses are involved against two different sovereigns (e.g., the state and the federal government). Certain elements exist in every crime. These elements are normally contained in the definition of the crime, and each element must be proven beyond a reasonable doubt for a suspect to be found guilty.

Both **intent** and act are necessary elements of a crime, and **they must occur at the same time**. In order for an act to be a crime, it must be done intentionally, not by accident or as an unconscious act. **Intent** is defined as the deliberate and willful resolve to do an act. It generally is an indispensable part of a crime. For example, one who is pushed by another and then accidentally bumps a third person over a cliff has not "acted" within the meaning of the law. And intent is **not** the same as motive.

Intent is the determination to do a certain thing; motive is the reason for doing it. An **act** is a willed performance of an action. Some crimes can result from **failure to act**, which is the omission or failure to perform a legally required action, such as feeding one's children. **Motive** is not an element of a crime.

**Statutes** are laws passed by legislative bodies. **No act can be a federal crime unless it is prohibited by and punishable by a federal statute (e.g., contained in the USC).**

Under the **Assimilative Crimes Act** (contained in Title 18, USC), a violation of state law in an area of federal exclusive or concurrent jurisdiction can also be a federal crime prosecutable in federal courts. In such cases the federal government assumes (assimilates) the state criminal code as part of the Federal Code.

**Common law** does not apply within the federal statute. It may apply however in the state/local statutes. **Treason** is the act of waging war on the United States, adhering to its enemies or giving them aid or comfort. **Felonies** are crimes that normally are punishable by a sentence of a year or more in prison. **Misdemeanors** are those crimes that normally are punishable by one year or less in prison.

### 3.2: Common Offenses

The most common offenses that you will encounter are listed below. They fall into three general categories: **unauthorized use of drugs and alcoholic beverages, property crimes** and **violent crimes**. You must know the nature of these offenses and likely offenders. You must be prepared to prevent, detect and report crimes that may be committed on federally-controlled property.

It is important that you understand that **you are NOT a sworn law enforcement officer**, even if you are deputized under current or past employment endeavors, you do not have arrest authority while performing on an FPS security contract. FPS does not expect and will not require you to perform the duties of a sworn law enforcement officer. **Unless there is a situation involving the imminent danger of injury, death or destruction to persons or property within your facility, and you have no choice but to act to minimize or prevent the com-**

**mission of a crime, you should always try to report to the FPS MegaCenter first, then act.** In instances where you are compelled to act, once you have taken action to control the situation, you must **immediately** report the situation to the FPS MegaCenter. Dispatchers/Operators at the FPS MegaCenter have instant and direct access to law enforcement, fire and the life safety/rescue activities in your area. When you report a situation to the FPS MegaCenter, they will dispatch the appropriate personnel to your facility. Dispatchers/Operators receive extensive training on dealing with a wide variety of incidents, and they act as a conduit to FPS and law enforcement.

### Unauthorized Use of Drugs and Alcoholic Beverages

One of the most frequently occurring offenses on government property is the unauthorized use of drugs and alcoholic beverages. People cannot enter federally-controlled property while under the influence of, using or possessing narcotics, hallucinogens, barbiturates or amphetamines (excluding medically prescribed drugs); or alcoholic beverages. Appendix 1, 41 CFR (102-74.400 & 405), Alcoholic Beverages and Narcotics, contains additional information.

The regulations regarding drug and alcohol possession and usage should be posted at entrances to federally-controlled facilities. If they are not posted, notify your supervisor, who then should contact the responsible FPS official. The head of the responsible agency may give approval for the use of alcoholic beverages on federally-controlled facilities for such occasions as retirement or holiday parties. When this approval is granted, you will probably receive a copy of a memorandum stating so which will be included in your duty book.

If you discover or are told about the unauthorized use of prohibited substances in your assigned facility, follow your post orders for handling such situations. If your post orders do not address this subject, report the situation to the FPS MegaCenter.

In most cases, FPS law enforcement personnel will be dispatched. **Do not** take action on your own, and discuss the issue with the appropriate officials only. Security guards are subject to the same restrictions. If found in violation of the regulations, using or in possession of drugs and/or alcohol while on duty, you will be subject to disciplinary action. You will

also face immediate dismissal from the contract and be prohibited from ever working in a federally-controlled facility.

## Property Crimes

Property crimes are those crimes that involve the theft, damage or destruction of property. As a security guard, you may be involved in responding to and/or reporting incidents of property crime. Property crime can be related to either government or personal property. It would apply to employees or visitors to the facility. While there are many types of property crime, the types you will most commonly deal with while on duty are **vandalism, larceny-theft, burglary** and **arson**.

These crimes are all prohibited by the FMR and are punishable under Title 18 USC. Appendix 1, 41 CFR (102-74.380): Preservation of Property contains further information.

### Arson

Arson presents a serious threat to the life and safety of building tenants and visitors. Arson is defined by the FBI/UCRP as any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle or aircraft, personal property of another, etc. Only fires determined through investigation to have been willfully or maliciously set are classified as arsons. Fires of suspicious or unknown origin are excluded. The FBI/UCRP reports that in 1999 there were over 75,000 reports of arson in the United States.

The motives of an arsonist and the evidence of the crime may be difficult to detect, as evidence is often destroyed by the fire. The instruments needed to commit the crime (e.g., matches, cigarette lighter, candles, etc.) and other flammable materials may be openly purchased and legally carried on the person. Consequently, an arsonist can pass undetected with the aforementioned items in his/her possession. An arsonist may not be deterred by the potential loss of life, or the dangers of fire fighting.

There is no foolproof system to help identify and account for every case of arson. Arsonists can be of any age, and their motives may vary. Fires may be set by people seeking economic gain, concealing a crime, taking revenge for a perceived wrong or as a

result of a dispute or grievance. This could involve a particular government agency and/or government employee. You must also be aware that the possibility exists that someone could intentionally start a fire to be the “hero” coming to the rescue of people that may be in the building, seeking personal recognition and congratulations.

Whenever there is a fire, keep the curious away from the site while awaiting response from fire officials. Once on site, the fire officials should determine when the area can be opened for public access. If specifically posted to an area for security purposes, follow whatever instructions you are given.

### Burglary

The FBI’s Uniform Crime Reporting Program (FBI/UCRP) defines burglary as the unlawful entry of a structure to commit a felony or theft. Forcible entry is not a requirement for a crime to be categorized as a burglary by the FBI/UCRP, although in many localities it is. You can contact your regional FPS law enforcement personnel for more detailed information on the local laws and jurisdictional issues on burglary.

Burglary is an act of stealth where the offender usually acts when no one is present to see the crime. Most often, burglars enter a facility by forcing open a window or door. Incidents of burglary increase when doors and windows cannot be properly secured and/or have no alarms, or when the security force is inefficient. In the late 1990s, there were over 2,000,000 reported burglaries each year in the United States.

There is no “typical” burglar. A burglar may be any race, nationality, gender or age. Burglars are generally classified within three types: **amateur, juvenile or professional**. **Amateur** and **juvenile** burglars can travel far looking for an opportunity to steal or may decide to steal on the spur of the moment if an opportunity presents itself. They usually will choose a place that is easy to enter with the least possible chance of detection. They may also cause needless damage in an effort to burglarize property quickly as possible. **Professional** burglars generally will plan their crimes more carefully and may conduct prolonged surveillance of an area prior to attempting the crime.

Items that are most sought after by burglars in federally-controlled facilities are computers (especially laptops), calculators and audiovisual equipment. Personal items may also be stolen during a burglary, especially if valuable and not properly secured in a desk or cabinet (e.g., jewelry, money, purse/wallet, etc.).

To reduce the chances of a burglary in a facility you are protecting, if you are assigned to a roving post, your patrols should be in accordance with your post orders. However, if able to do so, be careful not to set a consistent pattern by which anyone watching can time you.

Ensure you pay close attention to secured areas/spaces known to contain valuable equipment or property, checking windows, doors, locks and whatever else is applicable. If assigned to monitor the alarm system, be alert for any activations and report them immediately. If assigned to an access/egress post, ensure the proper identification checks are performed for employees, and the established access control procedures for visitors to the facility are strictly followed. Although statistically more burglaries occur in non-residential buildings at night, burglary can also happen during other times as well. You must be constantly alert to activities occurring in your facility.

Burglars should be considered extremely dangerous. Burglars want to escape detection and may use a weapon if caught. They may be extremely nervous and prone to panicking if discovered. Exercise extreme caution whenever responding to a possible burglary.

### **Larceny-Theft**

Larceny-theft is defined by the FBI's Uniform Crime Reporting Program as the unlawful taking, carrying, leading or riding away of property from the possession of another. It includes crimes such as shoplifting, pocket picking, purse snatching, theft from vehicles, etc., in which no use of force, violence or fraud occurs. In 1999, there were nearly 7,000,000 reported cases of larceny-theft in the United States. Aside from vandalism, this is by far the most common property crime you may encounter as a security guard.

When you are writing a report involving the taking of property without permission, you should describe it as larceny unless you have reason to believe there

was no intent to permanently deprive the owner of his/her property. Give any reasons and other evidence relating to intent, such as a statement by the suspect or an attempt to sell the stolen property.

An example would be if Mr. Doe takes Mr. Smith's calculator to do work in the office and forgets to return it, there is no larceny. Note that the calculator was not removed from the building.

If you are on a roving patrol, watch for people acting suspiciously. Take note of any government property being transported. Be alert for property that may be out of place (such as a computer in a utility closet). Any sighting such as this should be reported immediately. Thieves will frequently store stolen property in a temporary holding place until they can come back for it. If you are on an access/egress post, be observant especially of personnel leaving the facility. Any government property being taken out of the facility should be in accordance with the agency's accountability procedures and/or post orders.

### **Vandalism**

Vandalism is the act of willful damage of a property without the owner's permission. The term "damage" includes destruction, disfigurement or defacement. Damage can be inflicted by cutting, tearing, breaking, marking, painting, drawing, covering with filth or other actions prohibited by law or regulation. The property can be government-owned, public, private, personal or real (e.g., buildings and grounds).

Acts of vandalism range from child play that gets out of hand to intentional damage by an individual, or a group (such as a gang). There is no simple technique that can be used to prevent vandalism. However, frequent and aggressive patrols, or a visible security presence will discourage would-be vandals.

### **Violent Crimes**

While incidents of violent crime are much more infrequent than incidents of property crime in government buildings, you may be required to respond to instances of violent crime. As a general rule, you should always exercise extreme caution whenever you receive a report of a violent crime; as these are serious offenses that often involve weapons or the threat of force. Report and follow the instructions given to you in your post orders when responding.

Although there are many types of violent crimes, the ones you will most likely encounter while on duty are **assault** and **robbery**. These crimes are prohibited and punishable by Title 18 of the U.S. Code.

## Assault

Assault is defined in criminal law as an unlawful attack by one person upon another. Verbal threats do not constitute assault. Most cases of assault are not premeditated but instead usually arise out of a heated emotional encounter.

### Simple Assault

On occasion, it is the practice of local jurisdictions to charge an assailant with simple assault. It generally involves an assault without the intent to cause serious or mortal injury. The incident may or may not involve a weapon of some type. When responding to an incident of this nature you should exercise caution.

### Aggravated Assault

Aggravated assault is defined as an unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault usually is accompanied by the use of a weapon or by means likely to produce death or great bodily harm. (It is not necessary that injury result from an aggravated assault when a gun, knife or other weapon is used which could and probably would result in serious personal injury if the crime were successfully completed.) Aggravated assault is the most commonly reported violent crime.

## Robbery

The FBI/UCRP defines robbery as the act of taking or attempting to take anything of value from the care, custody or control of a person by force or the threat of force or violence, and /or by putting the victim in a state of fear. When a weapon is involved, the crime is armed robbery. In contrast to burglary, robbery always involves confronting another person and possibly being observed by many others.

Although robbery is not as common as burglary, it has the potential to be more dangerous because many robbers are armed and prepared to use their weapons if necessary. Many law enforcement officers have been wounded or killed by armed robbers.

Robbers usually plan their crimes and often have

accomplices. Professional robbery gangs will often use other criminals to obtain information about the intended victim or target. The accomplices will observe the activities of the potential target in exchange for some form of payment, but seldom participate in the actual robbery. The lone robber will act independently. Robbers will employ a variety of methods to flee from a crime, such as fleeing on foot or using various forms of transportation at their disposal.

As a security guard, you can help prevent robberies by remaining vigilant on duty. Pay attention to people entering the facility who may appear nervous or acting in a suspicious way. If the facility you are assigned to has an ATM and you are on a roving post, ensure you inspect the area as required according to your post orders particular on paydays and during the busy times of the day.

## Other Crimes

You may encounter crimes while on duty not mentioned in the manual but prohibited under Title 18 of the U.S. Code. Dependent upon the crime, and the situation you are presented with, your primary responsibility remains to control the situation, use as minimum force as necessary to do so, and report the incident as soon as possible to the FPS MegaCenter.

### 3.3: Reporting Incidents to the FPS MegaCenter

As a security guard, it is very important that you understand the necessity to remain in close contact with the FPS MegaCenter at all times, regardless of the situation you are presented. The National number for the MegaCenters is 1-877-4FPS-411 (1-877-4377-411).

If you are unsure whether a situation/incident should be reported, you can contact your supervisor for clarification. If no supervisor is available, your “action” should **always be** to report it. Once you have reported it to the FPS MegaCenter, you have done your required duty. As an example, you are on a roving post one day and observe what appears to be a disagreement between two employees in an office. As you approach you hear screaming and name-calling. However, once you enter the office and your presence is noted, all becomes quiet. You

make a mental note of it because you know the employees involved but you fail to report it to anyone. A few days later, security guards are requested to that same office for a reported assault. You soon learn the suspect and the victim are the same two employees you observed in an argument a few days back. During the course of the investigation into the assault, a co-worker informs the investigating officer of the argument you observed initially between the two. The FPS MegaCenter is contacted to provide information from the **report you should have submitted**. You have now brought unwanted attention upon yourself and will probably be asked why you failed to report the incident.

The dispatchers/operators of the FPS MegaCenter are there to assist you and to provide any support you need. You should never feel or think that by making a report you are “bothering” them or that what you are reporting is insignificant. Your responsibility is to report it, let the officials decide if it is significant or not. Your observations are very important. When reported, they may establish or add to a pattern that FPS officials can notice and act upon, thus maintaining or improving security in your facility.

For your knowledge, the following is a list (not all-inclusive) of the types of incidents or situations that you should report to the FPS MegaCenter:

- unusual, suspicious or disruptive behavior by an employee or visitor;
- objects (e.g., computers, projectors, etc.) out of place and unsecured;
- crimes;
- doors/windows found unsecured, possibly having broken locks;
- prohibited items (e.g., drugs, alcohol, etc.) in the possession of a person or found within the facility;
- any alarm activations; and
- any abnormal occurrences (e.g., an unusual odor, an argument between people, the smell or sighting of smoke, etc.).

Anything that does not “feel right” can be reported. The more experience you gain as a security guard, the more you will be able to distinguish when a situation should be reported. Usually security guards with experience become very comfortable with reporting to the FPS MegaCenter.

If there is ever an occurrence where you report to the FPS MegaCenter and do not receive adequate assistance, or if the dispatcher/operator is rude/unhelpful, get the name of the individual if possible and then report it to your supervisor. Your supervisor will contact the appropriate FPS official to investigate the situation. Just as it is expected of you to be courteous and professional in your duties, expect the same from the FPS MegaCenter dispatcher/operator.

### 3.4: Jurisdiction

**Jurisdiction** is defined as the physical or geographical area where police power can be exercised and outside of which police power cannot be exercised. It limits the authority of police to act. There are three primary types of jurisdiction: **exclusive**, **concurrent** and **proprietary**.

**Exclusive jurisdiction** covers areas where the federal government owns the property and has acquired all the law enforcement authority, and the state/locality where the area is located has not reserved the authority to act at the same time. However, if a facility is covered by exclusive jurisdiction, the state/municipality law enforcement officers still have the right to serve criminal or civil warrants for offenses that took place outside the federal area. They can also give “hot pursuit” onto the property. An example of hot pursuit is when local police are pursuing a suspect in a reported stolen vehicle. If the driver of the vehicle enters property with exclusive federal jurisdiction, the local police can still continue the pursuit and stop/arrest the suspect even on property covered by exclusive jurisdiction, since the crime occurred outside the property. Additionally, upon invitation of an authorized FPS official, local police officers may be invited onto property with federal exclusive jurisdiction to assist FPS law enforcement personnel. State/local police officers may enter the property with their weapons only in the course of official law enforcement business. In nearly every situation where a state/local police officer enters property covered by exclusive jurisdiction, a federal law enforcement officer will accompany him or her.

Exclusive jurisdiction is rare for federally-controlled facilities. It usually occurs on military reservations or property where there is a military police pres-

ence. It can also occur on property that was once owned by the military but was taken over by another federal agency and the exclusive jurisdiction was retained by the agency.

**Concurrent jurisdiction** applies to areas where the federal government owns the property but where both the federal government and the state/locality have agreed to exercise their respective police authority (e.g., FPS law enforcement personnel enforce federal laws and state/local police officers enforce state/local laws). In concurrent jurisdiction areas, local police officers may exercise all the police authority granted to them.

**Proprietary jurisdiction** applies to areas where the federal government has acquired some right or title to property (such as a lease), but the state has retained police authority. Many federally-leased facilities are covered by proprietary jurisdiction, and the state/local police are primarily responsible for exercising police authority. Federal law enforcement officers have limited authority to enforce federal laws on property covered by proprietary jurisdiction; their authority is specified under the applicable U.S. Code.

Your duty book will usually describe the type of jurisdiction that applies to your facility. While you may not need to know what type of jurisdiction your facility has, it can be helpful if there is ever a case where state or local police need to enter federal property to conduct their duties. If this occurs, the FPS MegaCenter should be notified.

### 3.5: Search and Seizure

The terms search and seizure usually are used together, but they do not have the same meaning. In legal terms, search implies “invasion and quest” to discover articles hidden from view. Seizure means to take something forcibly from the owner.

You can have a search that doesn’t end in a seizure and a seizure without a search. For example, items in plain view outside or inside a building to which you have been lawfully admitted may be seized because no search is necessary. This is called the “plain view” doctrine. According to the Supreme Court: “It has long been settled that objects falling in plain view of an officer who has a right to be in

the position to have that view are subject to seizure and may be introduced in evidence.” Further, there is no search when items are:

- discovered through accident;
- shown voluntarily by the suspect;
- found while conducting an inventory of a suspect’s property after his/her arrest;
- found while the items are properly impounded in the custody of police; or
- picked up after being discarded by the suspect.

You cannot stop just any passerby, even one near the scene of a crime or one with a criminal record.

**As a FPS security guard, you should never conduct a search or seize items without being specifically authorized to do so; having received orders from a FPS law enforcement official or if contained in your post orders. Without specific authorization, search and seizure will be conducted only by sworn law enforcement officers.**

If in the course of performing your duties you have reason to believe that a search or seizure is necessary, immediately contact the FPS MegaCenter to report the situation before proceeding. Normally, law enforcement officers will be dispatched, and your job will be to stop or detain the individual until the police arrive.

If your post is access control, processing personnel and their belongings through the x-ray machine and magnetometer **does not** meet the legal standard for search and seizure. Your process procedures should be in accordance with and not deviate from the post orders. Post orders are written so your procedures **do not** constitute a search or seizure. Ensure you are aware of the proper processing procedures to avoid creating a possible illegal search and seizure issue. For clarification, contact your supervisor and ask for assistance.

### 3.6: Detainment Authority

As a security guard you will probably deal with situations where people refuse to cooperate with access control procedures or behave in a disruptive, dangerous or possibly life-threatening manner. In such situations it may be necessary for you to secure the person’s presence until law enforcement

personnel can arrive to support you and take over the situation. This process is called **detainment**. As a FPS security guard, you are authorized to detain people if it is necessary to ensure order and safety at your assigned facility.

**You should detain a person only when absolutely necessary and with the minimum level of force necessary to control the situation.** The use of force parameters are discussed later in this manual. Your employer is responsible for ensuring you receive the proper training on the use of force and the various levels that apply. Additionally, your post orders will contain the proper procedures for handling personnel, which includes detainment and reporting.

You should be aware that using an “unreasonable level” of force to detain a person could result in a civil lawsuit being filed against you. An “unreasonable level” of force is defined as that level of force that is not appropriate to control a situation.

You must rely on your training, judgment and guidance contained in your post orders to determine what level of force is necessary when faced with having to detain a person. It is very important that you document the occurrence/situation with complete details. Your report should cover everything from beginning to end. This should be done as soon as possible while the information is fresh in your mind. If you are sued by an individual, your written report will be a valuable piece of information for establishing the facts surrounding the detainment incident.

**Whenever you are faced with a situation where, based on the facts, your judgment and guidance contained in your post orders, you believe an arrest is necessary, remember only a sworn law enforcement officer can make an arrest. You should contact the FPS MegaCenter immediately.**

Detainment is a serious act. Use your best judgment to proceed, and remember the FPS MegaCenter is there to support you.

### 3.7: The Use of Force

There may be times in your job when you will be confronted with situations that present a danger to you, other people or to federal property. When this happens you may need to exercise a degree of “force” to control the situation. It is extremely

important that you understand the different levels of force, when to use force and what level of force to use based on the situation.

The Federal Law Enforcement Training Center (FLETC) created a Use of Force model that is currently being taught to all FPS law enforcement personnel during their basic training. FPS strongly encourages all companies to use this model as a training guideline for all potential FPS security guards during their training. Ultimately, as a security guard, you will be responsible for determining when and how much force is necessary. A copy of the Use of Force model is incorporated into this manual, contained in Appendix 4. Report any use of force immediately to the MegaCenter.

Because the document is intended for law enforcement personnel, many of the examples given refer to arrest procedures. As previously stated, **an FPS security guard does not make arrests**. However, the principles outlined in the model still apply to you. You can use them because you do have the authority to detain a person if necessary.

Naturally after viewing the Use of Force model, you will question what is expected of you. You should remember, your first reaction to a situation is to get it under control. If use of force is necessary, you are expected to use the minimum level of force necessary. You will rely on your training, experience and judgment to determine the best course of action, keeping in mind that the safety of life and property is your first priority. If unable to contact the FPS MegaCenter prior to taking action, report the situation to them as soon as able to do so.

### 3.8: Crime Scene Protection and Evidence Procedures

When a crime occurs in a federally-controlled facility, you may be one of the first people to arrive at the scene. After assisting any injured people, ensuring the safety of all persons and property, and contacting the FPS MegaCenter to report the situation, one of your most important duties will be to ensure the integrity of the crime scene. This means maintaining it in its original condition. Law enforcement officials may direct you to protect the crime scene until law enforcement arrives, and possibly even while the scene is being investigated.



A **crime scene** is the area where the crime occurred. It can be as small as part of a hallway or room, or as large as an entire floor or building, depending on the crime.

When objects or people are touched, materials are transferred. Criminals may leave traces of evidence at the crime scene, such as fingerprints, footprints, bodily fluids, heel marks, etc. In fact, virtually any object, material or fluid can be or contain evidence. This evidence is called **physical evidence**, and it is important because it connects the suspect to the crime scene. The use of physical evidence in a trial will in part depend on it being effectively protected. The prosecuting attorney(s) must be able to show that the evidence was found at the scene, relates to the suspect, is connected to the crime, has not been changed and is distinguishable from other items.

To protect the crime scene while waiting for law enforcement personnel to arrive, take the following precautions:

- make sure no one touches, picks up or disturbs in any manner, any objects or materials within the crime scene area;
- allow no one to enter the crime scene area and change anything;
- if you must assist injured personnel, try to use a route that avoids contact with possible evidence and always use the same route;
- separate witnesses and victims; ask them to not discuss the incident among themselves and request that they remain available to be interviewed; and
- keep the area secured until properly released by law enforcement officers.

Because you are not a sworn law enforcement officer, you will not collect or process physical evidence. However, you should make detailed notes of what you observe at the crime scene for report purposes.

### 3.9: Testimony

Cases that result in arrest may lead to legal proceedings, such as a pre-trial conference, a hearing or a trial. You may be called to give testimony and make an important contribution to the proceedings. If you are called to give testimony, you may be contacted first by an attorney to prepare for the legal

proceedings. When you are contacted, make sure you notify your supervisor and FPS as soon as possible. The attorney will usually discuss why your testimony is needed, the types of questions you will be asked and how you should conduct yourself while under oath. Cooperate fully with the attorney and follow his/her advice. A copy of the subpoena requiring your presence at the legal proceedings should be submitted immediately to your supervisor and FPS.

If called to give testimony, you should carefully review all your notes prior to appearing in the proceedings. Remember that your personal appearance is very important—appearance impacts upon your credibility. Ensure your uniform is clean and pressed when you report to the proceedings. You will not carry a weapon or any other duty equipment (i.e., baton, flashlight, etc.) to the proceedings.

Your familiarity with the courtroom and the proceedings will allow you to relax and as a result, be a better witness. The attorney should explain all the specifics and procedural aspects to you prior to you being called for testimony. This should entail the various roles and functions of the proceeding's participants such as the prosecutor, judge, bailiff, etc. It should also entail your conduct under oath and on the stand as well. Remember, in legal proceedings you are representing your employer and the government. Your behavior and standards of professionalism are being looked at as well.

Page 28  
Left Blank Intentionally

# Chapter 4

## Security Guard Contract Administration



To be an effective security guard, you must understand the nature of the contract between your employer and FPS. This chapter will discuss that relationship as well as how you will interact with FPS and other federal employees. It will also review administrative requirements and discuss weapons and equipment you will use.

### 4.1: Your Job as a Security Guard

Since FPS needs to secure federally-controlled buildings to protect federal property, the occupying agencies and customers, FPS has established a contract with your employer to provide security guard services. To meet the requirements of the contract, your employer has hired you.

As a part of the contracting process, FPS issues a Statement of Work (SOW). The SOW lists those specific actions and services that must be provided by the contractor. For example, SOWs for security guard service contracts often specify requirements for post hours, uniforms and equipment and training and certification requirements for security guards. All the work that you will perform is based upon the contract requirements. Your employer is paid and the company's performance under the contract is evaluated based upon the level of compliance with the contract requirements. If there is conflicting guidance between this manual and the contents of the contract, your employer is responsible for ensuring the contract requirements are met.

### 4.2: Relationship between the Contractor and the Government

#### Working with DHS

Because you are working under a contract for FPS, you may be inspected by FPS personnel. Additionally, many federal agencies have personnel who have been designated as agency technical representatives (ATR) by FPS. ATRs have limited authority to observe the security guards and the post area. Their findings are reported back to FPS. It is possible you will have frequent contact with these individuals since they are normally located within the same facility where you are assigned. They may question you concerning your post, duties and authority. While on duty your chain of command consists of contacting your supervisor and/or FPS MegaCenter for any problems or situations. Inspections by FPS personnel are not designed to harass you or attempt to get you fired, but to improve upon the security services. If negative performance and/or conduct are noted, naturally it will be reported and your employer will be notified.

Whenever you receive a visit from FPS personnel or an ATR inspecting your post, you should request to see their identification/credentials for verification purposes. On your post contained within your duty book should also be a listing of FPS personnel and the ATR who may visit your post. If there is any doubt on your part pertaining to their identification or purpose, contact your supervisor or the FPS MegaCenter. Ensure you record their visit in your logbook. If the individual wants to make the entry, allow him/her to do so, and you can follow it up with your own remarks.

If while on duty you receive an inquiry from the media, you should contact the FPS MegaCenter. You are not authorized to represent the government in instances such as this and may not respond to any questions regarding agency or contract matters.

### Working with Occupant Agencies

You should always be professional, keeping a helpful and respectful attitude when dealing with employees of the federal agencies occupying the facility you are guarding. You must remember however, that you do not work for these agencies. You are contracted to provide services for FPS and in as such are provided post orders which detail your specific duties. An official of another agency cannot order you to deviate from your established post orders. If such an attempt is made, do not get into a heated discussion. Maintain your professional demeanor and contact your supervisor and the FPS MegaCenter immediately. No changes or deviations from your post orders are allowed unless you have received specific authorization from a representative of FPS.

### 4.3: The Post Duty Book

FPS provides a duty book at each of their guard post. It provides important information for the security guard on duties to be performed. Your knowledge of its contents is essential and every security guard should refer to it when necessary. Using the duty book will ensure all guards at that post are conducting business in the same manner. It will contain all current policies, orders/instructions, emergency procedures and any other information deemed pertinent for the facility. Incoming guards will read the duty book for any changes, additional information, etc. that may have occurred. The post duty book is divided into five parts, described below:

- **General Orders.** This section contains general information/guidance issued by FPS and applies to all posts. Information is usually listed in chronological order, the most current being on top.
- **Specific Orders.** This section contains information provided locally and applies to a specific post.
- **Special Orders.** Special orders are usually effective for no more than 60 days. The information is in chronological order, with the most current on top.

- **Emergency Instructions.** This section will contain the Occupant Emergency Plans and evacuation routes. It will also identify the location and procedures for emergency equipment shut-off valves or switches.
- **Access/Contact Lists.** This section will contain the applicable access list for the facility and the names and telephone numbers for employees of the tenant organization(s).

Changes to the duty book should come through your supervisor and/or the FPS MegaCenter. If applicable, advise your relief of any changes that occurred during your shift.

### 4.4: Work Schedules

Work schedules for supervisors and regular security guards are to be prepared separately. Your employer is required by contract to post a copy of the work schedules in an area accessible by you, such as your work area or locker/break room at regular intervals.

Your company may require you to attend roll call/guard mount prior to assuming duty. This is not a requirement by the government. This time can be used for training, information updates, inspections and any concerns you would like to discuss.

If this is your company's policy, your supervisor is responsible for ensuring all guards scheduled are present, all are in the proper uniform with all required equipment and all have their identification/certifications on their person.

Punctuality is of the utmost importance. Ensure you sign in and sign out in accordance with the proper procedures.

### 4.5: Weapons and Equipment

Weapons and equipment will vary for security guards according to your location. Not all guard service contracts require the same equipment. In addition to a firearm, the most common equipment you will use and become familiar with are the handcuffs, baton and radio. Regardless which equipment your contract may require, your employer is required to ensure you receive the proper training and certification in the usage and maintenance of the equipment.

## Firearms

If you are assigned to an armed post, you are authorized to wear only the firearm and use only the ammunition specified in your contract. Prior to being allowed to carry a firearm, you are required to complete and pass the firing range qualification course. This will allow you to be issued the necessary license/permit required according to the contract. Subsequent re-qualification is required annually to maintain a valid license/permit for carrying a firearm. Any security guard who fails to re-qualify or who allows his/her license/permit to expire will not be permitted to work on contract. It is your responsibility to monitor your expiration date(s) for weapons re-qualification and your license/permit. You will notify your supervisor when your re-qualification date is due within 60 days and again in 30 days if no action has been taken. This will allow time for your employer to arrange for your re-qualification prior to expiration.

Proper care and maintenance of your weapon is your responsibility. The weapon should always be cleaned with only the proper materials. Do not drop it, throw it or use it as a club or hammer. At your location, a regular schedule for cleaning the weapons should be instituted. When signing for your weapon, you should always inspect it and also the ammunition you will be using. If you can visually see or have reason to suspect the weapon has been damaged, or if it is unserviceable, notify your supervisor at once. The FPS MegaCenter should be notified also. Your supervisor and/or the FPS MegaCenter will give you instructions on what to do with the damaged weapon and also procuring you a replacement weapon.

### Firearms Accountability

Accountability for the weapon (and ammunition) is your responsibility once you have signed for it prior to assuming your post until you have been properly relieved and turn

the weapon back in. The weapon will be carried in accordance with directions provided in your post orders. Your post orders will also specify the confines/limits of your post.

You are not allowed to leave the limits of your post area or facility with your firearm unless specifically

authorized to do so by your post orders or other approved authority.

At some locations, security guards and supervisors are authorized to transport their weapon off federal property if required while on duty and provided their license/permit is valid. Refer to the post orders at your location for the proper storage and transporting procedures. You should also be aware that you will be held accountable for any negligent or criminal misuse of the weapon and subject to disciplinary action up to and including removal from the FPS guard service contract and possible criminal prosecution.

### Firearms Safety

Safety when handling/carrying a weapon is very important. Familiarization with the weapon is essential. You should always treat every weapon as if it is loaded. Improper handling, horseplay or just not being attentive, could all lead to an accidental discharge, which could result in injury to personnel and/or damage to property. The following is a list of some of the basic rules pertaining to firearms safety:

- keep your weapon holstered at all times and ensure the keeper strap is secured;
- never point a weapon at any person or cock the hammer unless justified in using deadly force;
- ensure when placing your weapon in the holster, you do not cock the hammer;
- never dry fire a weapon unless during the conduct of the range course or using an approved clearing barrel when clearing the weapon to be turned in;
- never leave a weapon unattended for any reason;
- never place your finger in the trigger guard unless intending to fire the weapon;
- ensure you follow the manufacturer's instructions when loading or unloading the weapon;
- never attempt to fire a weapon while running; and
- ensure you have the proper holster for the weapon.

As a security guard, your company is required to ensure you are properly trained in all aspects of the firearm you will be carrying while on duty. You should not be afraid to question your instructor on any issue/detail you are not comfortable with or do not fully understand.

You should be aware that in the event of a discharge, either intentional or accidental, your supervisor and the FPS MegaCenter must be notified immediately. If there is injury to personnel and/or damage to property as a result, follow instructions as stated in your post orders. You will make a written report as soon as possible while the circumstances are fresh in your mind. In the event of any type of discharge, FPS law enforcement personnel will be dispatched to your location to take possession of the weapon and ammunition.

## Handcuffs

Handcuffs are just one piece of equipment you are able to use if justified. You should consider using handcuffs when an individual is displaying erratic or violent behavior, which may cause disruption to the normal business routine of the facility, and could possibly jeopardize the safety of any persons present. In a situation such as this, you may be required to forcibly detain an individual until FPS law enforcement personnel arrive.

As with other equipment required by your contract, your company is required to ensure you receive the proper training/instruction in the usage of and proper application of handcuffs. During the course of training, ensure you ask the instructor any questions you may have and once performing your duties, you can ask your supervisor about any detail you may have forgotten or may not be sure of.

As a security guard, you should not use your handcuffs as a weapon and when they are not in use, they should remain in the carrying case on your belt.

## Baton

**The baton is to be used as a defensive weapon only.** Use it to temporarily disable a violent opponent. You must always justify the use of the baton. **Never** draw your baton unless you intend to use it and **never** strike any part of the body with the baton that may cause serious or fatal injury unless **deadly force** is authorized. Areas that may cause serious or fatal injury are the head, face, throat, chest, spine, kidneys, joints or armpits. You are authorized to use only the baton issued to you if required by your contract.

In the event you have to use the baton while on duty, as soon as able to do so, you will notify your supervi-

sor and the FPS MegaCenter. You will also be required to complete a written report explaining the incident.

As previously mentioned, you are required to receive the proper training/instruction from your company on the baton prior to being authorized to carry it on duty.

## OC/Pepper Spray

Within the Use of Force model, OC/pepper spray is classified as an “intermediate” weapon available to the guard and is used to temporarily disable a violent opponent rendering them incapacitated. All security guards will be properly trained in the use of OC/pepper spray.

## Radios

The Federal Communications Commission (FCC) and The National Telecommunications and Information Administration are responsible for assigning and enforcing rules and regulations governing the use of radio frequencies. These rules apply to all users of radio frequencies, including government and police departments. You should always follow the manufacturer’s instructions for use of the radio. The main parts of the radio are:

- **On/Off/Volume**—turns the radio on and off, also adjusts the volume.
- **Squelch**—will control the radio’s sensitivity.
- **Antenna**—necessary for transmission receipt. Be sure it is not broken.
- **Battery**—the power source. Charge it only as instructions state.
- **“Lollipop” Microphone**—If equipped with the hand “lollipop” microphone, do not clip it to the antenna.

Before using the radio on duty, plan/have an idea what your message will be. Ensure you listen for other transmissions before you attempt to make one to avoid “stepping” on someone else’s. You should receive proper training by your company on the radio depending on the type you have at your location. The training you receive should cover all the procedures for sending a message, receiving a message and troubleshooting issues. As a rule you should try to keep all transmissions as short as possible. If a message is long, try using the telephone as an alternate means.

When spelling or using letters in messages, use the phonetic alphabet. You should first state the letter, followed by its identifier, such as “A—Adam” or “B—Baker.” Never come across saying “A as in Adam.” The following is the phonetic alphabet list with the applicable identifiers:

<b>A</b> —Adam	<b>J</b> —John	<b>S</b> —Sam
<b>B</b> —Baker	<b>K</b> —King	<b>T</b> —Tom
<b>C</b> —Charles	<b>L</b> —Lincoln	<b>U</b> —Union
<b>D</b> —David	<b>M</b> —Mike	<b>V</b> —Victor
<b>E</b> —Edward	<b>N</b> —Nora	<b>W</b> —William
<b>F</b> —Frank	<b>O</b> —Ocean	<b>X</b> —X-ray
<b>G</b> —George	<b>P</b> —Paul	<b>Z</b> —Zebra
<b>H</b> —Henry	<b>Q</b> —Queen	
<b>I</b> —Ida	<b>R</b> —Robert	

When using numbers, they should be transmitted individually. For example, 1234 should be transmitted as “one-two-three-four,” not as “one-thousand, two-hundred, thirty-four” or “twelve, thirty-four.”

When transmitting descriptions of subjects, address the following: name (if known), gender, race, age, height, weight, hair color, eye color, complexion, scars or other prominent marks, clothing color, if the individual is armed, the type of weapon if known and, if moving, the direction and mode of travel.

When transmitting information about vehicles, use the following acronym: **CYMBL**— which stands for: color, year, make, body style and license number of the vehicle.

If required to use other codes such as “10” codes, for radio communication, you will receive the applicable training on same prior to initiating their usage and a copy of them will be incorporated into your post orders.

## 4.6: Posts

A **post** is an area of responsibility. A post can be “fixed” or “roving.” A fixed post can be located at an access control point, an information desk or a loading dock for a facility. Typical duties for a fixed post are as follows:

- observing all personnel at the respective access/egress points of the facility;
- inspecting packages, containers or briefcases;
- daily access control operations for employees and visitors;
- logging significant events in the officer’s operation log;
- review of the duty book for applicable orders/directives;
- contacting the supervisor or FPS MegaCenter as required;
- reporting any emergencies, alarms, etc., for dispatch of security guards; if on a fixed post, you will not abandon your post for alarms, calls, etc., unless within the limits of your post; and
- maintain overall security and protection for personnel, property and the facility.

Your roving post will cover the areas otherwise not protected by a fixed post or requiring a large number of fixed posts depending on location. The rover is mobile and can be on foot or in a vehicle. The security guard assigned as the rover will in most instances be responsible for responding to any emergencies, calls for assistance or alarms. Typical duties include periodically checking the facility perimeter, interior spaces or the garage.

Constant and attentive observation is necessary while working at any assigned post, fixed or roving. Always be aware of your surroundings and the people around you. The more familiar you become with the facility and surrounding area, the easier and more efficiently you will be able to notice something out of place. A few examples of things to look for are:

- suspicious packages left lying around;
- the various types of delivery trucks, vans, etc.; pay particular attention to one that has no type of markings or logo;
- entrances into the facility that are accessible from the outside;
- broken or malfunctioning perimeter CCTV cameras;
- people loitering around the facility;
- people pretending to be lost, misplaced and asking questions about the facility and/or
- people taking photographs.

## 4.7: General Response Procedures

Calls for assistance may come from an employee, a visitor to the facility or another security guard. Your response to any calls for assistance will be handled in accordance

with your post orders. Most of the calls will normally be “non-emergency” in nature, but all should be handled as if they are important.

An emergency call could be someone whose life is in danger, or the reported smell of smoke from within an office space or closet, for example. Procedures for emergency situations are contained within the post orders. In the event of a life-threatening situation, you should be current on first aid, CPR and the AED. You should also be familiar with the building layout so you’ll be able to proceed in the most direct route to the space/area where the person(s) are located.

If a crime has been committed and the suspect is fleeing, you may have to pursue. If possible, you need to notify your supervisor and/or the FPS MegaCenter before initiating pursuit. If unable to do so, report to them as soon as possible. Remember, you are not allowed to pursue anyone off federally-controlled property unless you have received authorization from FPS to do so.

As a security guard, there are a myriad of calls you could receive such as a theft, vandalism, suspicious person or an altercation. You are guided by your post orders, your supervisor and the FPS to handle any and all of these situations.

## 4.8: Emergency Plans

Emergency plans are a required component for every facility. Every facility will have a Building Security Committee (BSC). The BSC consists of representatives from each agency housed in the facility and representation from Security, Medical and Property Management. Each building must have an Occupant Emergency Plan (OEP), and it is the responsibility of the BSC to formulate the plan. This plan is to assist the agency(s) in responding to all emergencies such as fire, bomb threats or natural disaster. The plan is specifically designed to facilitate a smooth evacuation or shelter-in-place if necessary, and to account for the personnel. FPS security

guards have specific duties to perform once the emergency plan is implemented. A copy of the OEP will be incorporated into the post orders for each facility. Contained in the OEP is a listing of personnel designated to direct the emergency procedures. They are identified as follows.

- The **Designated Official** is the highest ranking official of the primary occupant agency. This responsibility can be delegated to an alternate high ranking official if all occupying agencies of the facility are in agreement. This individual is responsible for deciding courses of action when faced with an emergency situation.
- The **Occupant Emergency Coordinator (OEC)** will implement the plan of action once the decision has been made. As a member of the command element, personnel will report to the OEC during emergency operations. The OEC is also normally the chairperson for the Building Security Committee. The OEC will see to the staffing needs of the emergency organization and arrange the training necessary for personnel occupying key positions.
- The **Floor Team Coordinator** has the responsibility for overseeing, expediting and controlling the evacuation of all personnel from floors within the building. Floor monitors will report to this individual. This individual will also coordinate any bomb searches if necessary.
- The **Floor Monitor** is responsible for overseeing and coordinating the evacuation of his/her assigned floor. This individual will have personnel designated as **area monitors** to check assigned areas for total personnel evacuation, overseeing evacuation routes and conducting bomb searches. The area monitor will report to the floor monitor once their mission has been accomplished. Your **handicap monitors and stairwell monitors** will coordinate with the floor monitor also.
- The **Medical Coordinator** trains and equips personnel assigned to provide medical assistance and supervises first aid or medical self-help.
- The **Damage Control Coordinator/Team** will normally be personnel from the Building Management Office. They will assist in controlling the emergency, will control/terminate the facility’s systems, assess damages if any and restore the building to normal operations.



Normally as part of the OEP, there will be an area (ideally an office space), designated to be the command post. This is where the designated official and other members of the command team will operate in the event of an evacuation. It should have some form of communication asset within, meet the requirements for fire safety and be large enough to accommodate the command team.

You cannot plan for each and every emergency that could happen, be it an earthquake, terrorist attack or some other natural disaster. Become familiar with your facility, your post orders and the contents of the OEP, which will assist you in performing your expected duties in the event of an emergency. As always, the FPS MegaCenter is there to provide support and assistance also.

Page 36  
Left Blank Intentionally

# Chapter 5

## Controlling Access and Egress

The purpose of controlling access and egress to a facility is to ensure that only authorized personnel, vehicles and materials are allowed to enter, move within and leave the facility. This provides the protection for all personnel and property within, and the facility itself. Security guards, by their presence and professional performance of duties, will discourage, detect and detain potential violators. People associated with criminals/criminal activity tend to avoid facilities and/or areas where there are professional security guards on site.

### 5.1: Why Control Access and Egress

Your duty as a FPS security guard is to protect the people who work in and visit federally owned/or controlled facilities and government property contained within. With effective access and egress control, this can be accomplished daily. Effective access and egress control will prevent personnel or material with the potential to cause damage from gaining entry into the facility. It will also prevent personnel from leaving the facility with equipment/materials not authorized to be taken out.

Access and egress is controlled by you as security guards and by equipment such as locks, intrusion alarms and the appropriate sign-in/out logs. Security measures will vary according to the area/location and type of facility. Some buildings will have the potential to be a greater target than others based on the agency occupying the facility. Levels of access/egress control will be set accordingly. In all cases, you as a security guard will be the primary deterrent.



### 5.2: Personnel Control

Several categories of personnel will require access to and be permitted egress from federal facilities. These include government employees, contractors, emergency personnel and visitors. Local procedures guided by your established post orders, should facilitate a smooth operation for all personnel concerned whether entering or departing.

The procedures in place for your facility should present a feeling of “safety” and “security” as well as discourage potential unauthorized personnel from attempting entry.

There are several procedures for managing entry to a building or area. Open access and egress is used for buildings or some internal areas where there is no need for control, and people may come and go as they please. In areas where access control is needed, there are several procedures established according to location such as:

- presentation of a valid, approved photographic identification (e.g., drivers license, military card or an agency produced access badge);
- an agency provided access list with names of personnel authorized entry used in conjunction with a valid photo identification;
- personnel allowed access with the proper photo identification but requiring an agency sponsor/escort for entry; and
- some personnel have been issued “key cards” which will allow them access via a locked door, turnstiles or other protected/secured areas (if on a post where access is allowed with a key card, you may still be required to check the individual’s identification).

Facilities should have 100 percent screening for all visitors. Most locations will require personnel to walk through the magnetometer and all possessions to be processed through an x-ray machine. The machines are not for harassment, but for safety, and are designed to detect the possible presence of weapons, incendiary devices or other prohibited items/material. You will also visually check other items such as laptop computers and cellular telephones.

During the screening process it is important to be familiar with the beliefs and customs of different cultures/religions. Visitors to the facility may be dressed in cultural or religious garments and/or be in possession of religious articles. The following considerations will be afforded while conducting a search of someone wearing or carrying cultural or religious articles:

- show respect to all variations of faith during inspections;
- explain why you need to conduct a security search;
- if possible, searches should generally be conducted by a guard of the same gender; and
- if necessary and available, a private room may be offered for the search to be conducted.

Being culturally aware may prevent embarrassing situations and will portray the government in a positive light. Further guidance may be found in your general orders.

In the event an individual sets off the alarm walking through the magnetometer, you will first ensure he/she has removed all metal objects from their person. You will instruct the person to walk through again. If the alarm sounds again, you will use your hand-held wand if available to pinpoint the location of the metal material. You should be aware that sometimes a person may be wearing steel-toe boots, perhaps a belt with metal embedded in it, or even metal body parts that have been implanted surgically, any of which may cause the alarm on the magnetometer to sound. If in doubt or unsure in any situation, contact your supervisor.

During emergency situations, it may be necessary to admit law enforcement, fire or medical service personnel immediately into the facility. In these instances, your supervisor or the FPS MegaCenter should already be aware of the situation.

Once the normal control procedures for employees or visitors have been met, entry into the facility may be allowed. Visitors may have to be issued visitors' passes and/or escorted. If a person refuses to comply with the established procedures for entry into a facility, he/she will not be allowed access. In instances such as this, your response as a security guard will be dependent upon the individual's actions. Refer to your post orders for further guidance.

### 5.3: Property Control

Just as personnel are required to meet security requirements for access/egress of a federal facility, the same applies to property being brought in or taken out. An effective property control program will prevent theft, sabotage and other possible criminal activity.

According to 41 CFR- 102.74 (FMR), all federal facilities should have signage posted at entrances making personnel aware that all "property and/or belongings being brought into the facility are subject to being inspected."

Property could belong to the government or it could belong to a private person. There are several means by which property can be brought into a facility. It can be brought in by an employee or visitor, it can be delivered by courier, or it can be delivered by a company such as FedEx or UPS.

Incoming property belonging to individuals will be X-rayed in accordance with local procedures. Property being delivered for the government or a private party should be specifically addressed. These items will be x-rayed before being permitted to leave the access point. Property too big to be sent through the x-ray machine will be manually checked by a security guard. If possible, contact the recipient and have him/her present when doing so. Do not allow anyone to leave any packages unattended at your post or the surrounding area.

Outgoing government property will be accounted for before leaving the facility. Individuals removing government property from a facility should have a property pass signed by the appropriate authority. There should be a list of approved personnel along with their signatures contained in the officer's duty book. If in a building where the property pass is not

used, there should be specific instructions in your duty book/post orders. Some agencies no longer use the property pass and allow their employees to use their access badges or credentials as authority to remove property. In this event, property removed should be recorded in the guard operations log.

Each facility should also have procedures in place for accountability of lost and/or found items. Items turned over to the security guards should be annotated in a log to include the disposition of said item(s).

If any found materials/items are known to be illegal or prohibited, or if you are unsure about what has been found, contact your supervisor and the FPS MegaCenter immediately. Ensure a written report is made with the materials/items listed on it for any and all materials/items you are directed to seize.

#### 5.4: Vehicle Control

You may be responsible for controlling traffic in and around your facility. If so, your job is to prevent traffic congestion and deter criminal activity in parking areas. You may also be assigned as a parking control officer. This involves directing traffic into authorized parking areas and/or locating and reporting illegally parked vehicles. You may be required to wear and use specific equipment such as a reflective vest and a mirror for viewing the undercarriage of a vehicle.

In most cases, you do not have the authority to enforce traffic laws, rules or regulations. Consequently, if you become involved in an incident that requires law enforcement, for traffic issues or other criminal infractions, you will contact the FPS MegaCenter to report the situation immediately, and they will dispatch law enforcement officers if required. Dependent upon your location, you may be authorized to write “courtesy” citations as part of your assigned duties. Do not attempt to take this authority beyond what it is. You will receive training on writing citations and therefore should know exactly what to do. Your post orders and/or duty book contains the proper procedures and specific instructions on this.

You may be responsible for controlling entry and departures of vehicles from an authorized parking

area/garage. If required to inspect vehicles as part of access control procedures, the following general procedures may apply:

- stop the vehicle and advise the occupant(s) of the reason for the inspection;
- some locations may require the occupant(s) to vacate the vehicle; if so, check their identification and request they stand approximately six feet from the vehicle;
- conduct a thorough inspection of the interior, paying attention to areas such as between/under the seats, the glove compartment, above the sun visor and the trunk area; if alone on this post, remain attentive to the occupant(s) while conducting your search;
- inspect the exterior, as well focusing on the wheel area, behind/underneath the bumpers and the undercarriage, which will require the usage of angled mirrors that should be provided for you;
- if no prohibited items are found, thank the occupant(s) and allow them to re-enter the vehicle and proceed; and
- if prohibited items are found, detain the vehicle occupant(s) and contact your supervisor and the FPS MegaCenter immediately; follow procedures as outlined in your post orders.

#### 5.5: Lock and Key Control

Lock, key and card access control is normally provided by GSA in conjunction with the tenant agencies. If, however, security guards are required to maintain control of locks, keys and access cards, there should be an effective program for the control and accountability of these items, such as:

- a cabinet/container to hold all keys, or access cards tagged to identify which lock or reader it opens;
- a key/card access register with a list of information to be recorded;
- a list identifying keys/access cards and who are authorized to sign them out; and
- written procedures for the lock and key program.

If your post is responsible for maintaining controlled keys or access cards, you should at the beginning of your tour of duty inventory and account for all

controlled keys or cards. Once satisfied all are accounted for, sign the log acknowledging your inventory. Refer to your post orders for specifics.

There should be a guard equipment control register located on post. For every instance a key is issued or received, it should be recorded in the log. Controlled keys should be issued only to those approved personnel on your list who should be in the duty book on post. Although you may recognize employees, you are still required to request and verify identification.

If a controlled key/card is designated for “emergency use,” two copies should be kept in separate sealed envelopes with the outermost envelope marked “Open for Emergency Use Only.” The envelope should be signed and dated by the individual sealing it. This envelope should be kept separate from the other keys. If the need arises for the envelope to be opened, it will be recorded in the log and after the keys have been returned, the envelope resealed, signed and dated. Since these are designated for “emergency use,” ensure you issue them to only approved personnel.

All keys/cards maintained under your control are to be used in the performance of official duties only. Unauthorized use of these keys may subject you to possible disciplinary action.

# Chapter 6

## Intrusion, Detection, Assessment and Response



Detecting unauthorized access is a key function of a security guard. Advances in technology have provided a variety of security systems for use in federal facilities to assist security personnel. Intrusion detection systems (IDS) and closed-circuit television systems (CCTV), provide an additional layer of protection. They report to and/or alert security personnel, and allow remote assessment of the situation via monitors. While the detection function is less reliant on human sensors, you are still the primary means of alarm assessment and response.

### 6.1: Means of Detecting Intrusions

Detecting unauthorized access as a security guard means using your eyes, ears and hands as if a sensor. A security guard performing roving duties should continuously be looking for any broken windows, unlocked doors, open skylights, holes in fences and other signs of access into the facility or perimeter area. You will watch for unauthorized personnel in controlled areas either during normal business hours or after hours. Listen for any sounds or noises out of the ordinary. You will also check any security equipment you come upon during your roving duties ensuring that all equipment has been activated and is operating properly. Any suspicion of possible intrusion, attempted intrusion, malfunctioning equipment, etc. should be reported immediately to your supervisor and the FPS MegaCenter in accordance with the procedures in your post orders.

Depending on location, some security guards use the portable watchman reporting system to ensure the guards are performing the required patrols. The system is merely a clock with a key that allows the time and location to be recorded when used at a

station. A wired reporting system is also used which is like a key activated call box that reports directly to the FPS MegaCenter when used.

As mentioned in the introduction, today's technology provides a variety of security systems used to assist/augment the security guard. Some are listed below.

- **Electronic Intrusion Detection System (IDS)**—in common language referred to as burglar or security alarms. An IDS can be activated manually or automatically. An IDS system would consist of sensors, incorporate signal transmission lines, a monitoring board and fail safe features. It is generally employed to protect area perimeters on the exterior or open spaces, large areas in the interior or sensitive rooms/areas.
- **Electro-Mechanical Systems**—referred to as point sensors. These sensors detect the sound of breaking glass and an alarm results. Magnetic or mechanical switches can be installed on doors and once set, when the door is opened, the switch will be activated and an alarm will sound.
- **Motion Detectors**—can be ultrasonic, microwave or infrared and are designed to detect intruders in open areas. The ultrasonic and microwave sensors will transmit signals like radar, which bounces off walls, floors, ceilings and objects. The infrared sensor will detect changes in the temperature pattern of an area.
- **Audio Sensors**—are basically microphones in a protected area. Any unusual sound picked up will trigger an alarm.
- **Duress Alarms**—referred to as “panic buttons.” The one type of alarm with which most security guards will be familiar. These are activated by the simple pressing of an obscure/hidden button.

Signals from the sensors are sent to the FPS MegaCenter or designated central monitoring station that continually processes the signal. The control unit (which controls sensors for a zoned alarm area), then sends a signal to the system monitoring unit located at a post, control room or command center. The monitoring stations are manned by monitoring personnel.

If an alarm is received, it may be displayed visually on a console, map, diagram or computer screen. An audio alarm such as a bell or siren may go off, or lights in the area of the alarm may go on. For obvious security reasons, monitoring stations are usually in protected areas.

## 6.2: Assessing Possible Intrusions

If the alarm sounds locally (in your area), you may be the only security person on site aware of the alarm. Even though the alarm may register at a separate monitoring location, you shall immediately contact the FPS MegaCenter upon alarm activation. The monitoring personnel can look at their console or computer display and should be able to tell you if the alarm is a result of a door/window being opened or maybe a motion detection sensor in a secured area was activated. In any case, the information received will assist you in deciding how to respond to the area.

When assigned to a facility, you should educate yourself on the following aspects to aid you in assessing intrusions:

- where alarm systems are located and how they are deployed;
- the type of sensor(s) installed. Pay particular attention to where “detection” sensors have been placed; and
- if the alarms are tied into the FPS MegaCenter or a central monitoring station, which could tell you what sensors have been activated in a particular area.

Knowledge of the alarm system(s) in place is valuable information. When assessing a possible intrusion, there are other questions you should ask yourself such as:

- if a door/window alarm activation, are you familiar with the area?;

- if a motion detector activation, is it confined to one space or a large general area?;
- if a duress alarm, were you aware of personnel still in the area? What is the most direct route to them? Is there a telephone in the area where you could call to see if the button was pressed in error?;
- is there a means the intruder would know he/she has activated an alarm?; and
- have multiple alarms been activated by different means?

The CCTV system is even more apparent and present at most facilities.. A functioning CCTV system will enable you as a security guard to view perimeter areas (interior and exterior), access/egress points and any other areas deemed important enough to have it under remote surveillance. Your CCTV system can assist you in some cases when there is an alarm activation. Real, on-site surveillance is at your fingertips if the alarmed area is covered by CCTV. It will assist you also in determining a false alarm or if a response is necessary. Your CCTV system will also be connected to a video recorder so any activities may be recorded.

## 6.3: Intrusion Response Procedures

There must be a response to all alarms to determine if an actual incident occurred or if there has been a false alarm. Dependent on post orders, locations using CCTV systems may allow assessment based on remote surveillance, and no response would be required. Your duty book would provide specific guidance in these instances. The following information should be used as a guide when responding to an alarm:

- make sure your supervisor and the FPS MegaCenter are aware you are responding;
- maintain constant radio contact;
- treat all alarm responses seriously; you do not know if the intruder(s) are still in the area;
- make sure you have all of your equipment and it is in working order before responding;
- review all applicable information on the alarm system; the type of alarm activated could determine your response technique;



- approach the area cautiously; if necessary to enter an enclosed area, visually check the outside thoroughly before entering; conduct a thorough search once inside;
- if evidence is present, do not disturb it if at all possible;
- report in once you have completed the search and get instructions on how to proceed before departing the area;
- if the alarm is a duress activation it would normally mean an employee or fellow security officer is in trouble;
  - respond as quickly as possible; your actions when arriving on scene are important and could determine the outcome of the situation;
  - ensure you follow established procedures directed in your post orders;
  - contact your supervisor and the FPS Mega-Center as soon as possible and report the situation.
- Follow your post orders when responding to any alarms.

Page 44  
Left Blank Intentionally

# Chapter 7

## Facility Safety Procedures and Response



Protecting life and property is one of your primary duties. A major task is to detect conditions that can lead to fires or other serious safety issues, and to respond effectively if one occurs.

### 7.1: The Basics of Facility Safety

While working your assigned post, whether fixed or roving, you should always be on the lookout for any safety hazards/issues (e.g., slippery floors, leaky pipes, loose tiles or bricks, electrical shorts, loose door handles, etc.). Normally, the building management personnel should ensure any safety hazards are corrected and the proper inspection and maintenance is performed. You can check things like light bulbs, the automatic sprinkler system valves and fire extinguishers. If deficiencies are found, report them immediately to your supervisor and/or building management personnel. The FPS MegaCenter can be contacted also in the event the safety hazard is not corrected and an accident or injury occurs.

Some facilities will have specific areas to be checked where potential safety hazards may exist. Some of these areas are;

- storage rooms, closets and lockers;
- computer/server rooms;
- boiler rooms;
- restrooms, paying particular attention to toilets and sinks;
- crawl spaces, particularly under buildings;
- areas where smoking is prohibited. Look for cigarettes not properly put out;
- electrical closets for worn/defective wiring; and/or
- heat or flame producing equipment left on and unattended.

Familiarity with the facility will assist you with safety issues and response procedures. Attempt to acquaint yourself with the building layout and specific areas within or around the outside perimeter. Be aware of the following:

- the existing fire regulations;
- specific areas where flammables/hazardous materials may be stored;
- location of fire extinguishers;
- if required, the main shut-off switches/valves for the building's various systems;
- location of first aid equipment; and
- contact name and telephone number of agency representatives, and building officials for emergency notification.

Your building's OEP will also contain instructions. It should be located with your post orders.

### 7.2: Fire Alarm Systems

To assist you in understanding the fire alarm systems and the process once an alarm has been activated, knowledge of the basic principles would be helpful.

The three main parts of a fire alarm system consist of a **control unit**, **initiating devices** and **indicating devices**.

The **control unit** checks essential circuits, accepts alarm signals and provides power to the indicating devices.

The **initiating devices** detect fire and send a signal to the control unit. They include manual stations (pull boxes); ionization smoke, photoelectric smoke, flame and sprinkler water detectors; and sprinkler system supervisory devices.

The **indicating devices** provide the alarm to warn building occupants. Most signals are either bells or horns, and strobe lights to alert the hearing impaired.

Most of your facilities will have a fire control room, accessible by building management personnel, located on the property. Located in the front entrance/lobby areas for buildings will also be an “enunciator panel” which will show where the alarm has been activated.

### 7.3: Response Procedures

In the event of an emergency, you should take the following actions:

- determine the nature/type of emergency and contact your supervisor and the FPS MegaCenter immediately;
- if applicable, secure the immediate area from personnel;
- if a minor fire, attempt to extinguish it before it spreads;
- if necessary, contact the emergency response/life safety personnel;
- contact building management personnel if necessary;
- under no circumstances will you evacuate the building unless directed to do so by competent authority; and
- be prepared to do a written incident report.

You will have your post orders to refer to for guidance. More than likely, once you have contacted your supervisor and/or the FPS MegaCenter, you will be given instructions on what to do.

### 7.4: Knowledge and Use of Fire Extinguishers

Knowing where fire extinguishers are located in the facility will lessen response/reaction time in the event of a fire. There are three classes of fire:

- **Class A** fires are ordinary combustibles, such as wood or paper;
- **Class B** fires are natural or bottled gas, gasoline, paint and grease; and
- **Class C** fires are electrical equipment or wiring.

The following types of extinguishers are operated and used for the class of fire as noted:

Extinguisher Type	Operating Method	Class of Fire
Stored pressure	Pull out ring, squeeze lever	A
Water pump tank	Pull handle, squeeze, release	A
Carbon dioxide (CO <sub>2</sub> )	Pull out ring pin	B,C
Dry chemical	Pull out ring pin, squeeze, release	B,C
Multipurpose dry chemical	Squeeze, release	A,B,C

### 7.5: Acts of God or Other Serious Situations

This manual cannot possibly address every potential situation that could occur. For example, a tornado, earthquake, mudslide or a flood may happen at any time depending on the location and time of the year. Some natural occurrences are more prevalent during certain seasons. In any event, they may cause serious disruption to normal operations, and present problems for security and/or overall safety. As a security guard, if on duty when one of these occurrences happens, you may be required to stay until it is over.

In such an event, your primary responsibility remains the overall protection and security for personnel, property and the facility, although you may be forced to detour from normal operating procedures. It is quite possible you may have to act independently until assistance arrives. It is these times where you should rely on your training and judgment to perform your duties. If able to contact the FPS MegaCenter, you will be provided with instructions on how to proceed. If unable to contact the FPS MegaCenter, refer to your post orders, your past experiences and professional judgment. Maintain a continuous effort to contact the FPS MegaCenter. The operator/dispatcher will be coordinating response efforts, so your information and assessment of the situation at your location will assist him/her to prioritize their response efforts.

The situation at hand will dictate your actions and/or decisions. Regardless, your ability to remain calm and professional will be paramount. Focus on your daily routine, your past training and be confident in your abilities to accomplish your mission.

# Chapter 8

## Records and Reports

The ability to accurately complete forms and reports is an important skill for you to possess. This is known as report writing. Taking notes, completing forms and keeping records are essential tasks. These documents record information that may be used to arrest a criminal, used at trial proceedings, to record problem areas or incidents or to establish accountability.

### 8.1: Signing In and Out

Your employer is just one of many companies contracted to provide security guard services to DHS. For verification of your attendance and hours worked, you will be required to sign in and out on a modified version of DHS Form 139 (Record of Time of Arrival and Departure from Buildings). Because the government uses this form as a basis for payment to your employer who in turn, pays you for services rendered, it becomes very important that you fill it out correctly and accurately. Note that there is another version of Form 139 used for visitors signing in and out; do not get them confused.

The top of your Form 139 has three blanks entitled “Building,” “Year” and “Month.” These must be filled out on every sheet. In addition, the following columns should be filled out as indicated:

- **Date**—Self-explanatory.
- **Name**—Print last name, first name, middle initial.
- **Signature**—Sign first name, middle initial, last name.
- **Agency/Firm**—Leave Blank.
- **Room Number**—Leave Blank.
- **Purpose of Visit**—Leave Blank.
- **Arrival**—Record the exact time you start your tour.  
**Use the 24-hour clock.**

- **Departure**—Record the exact time you end your tour. **Use the 24-hour clock.**

Note that you should not sign out until you are actually departing. If you leave the site, you are required to sign out.

If you are in a supervisory position or on a roving post that covers several buildings, you must sign in and out at each building. As long as you take the most direct route between buildings, you are not off site.

There are additional simple rules to follow when signing the form:

- always sign on the next available line; do not skip lines.
- never ask another person to sign you in or out;
- never personally sign another person in or out;
- if a mistake is made on the form, cross out the entire line once, initial it and make the correct entry on the next line below; notify your supervisor of the mistake so he/she can initial it as well if there is no problem with the mistake made;
- do not forget to sign in and/or out; if you do so, it could lead to your pay not being accurate or you not being paid on time; and
- always record your correct times of arrival and departure.

Note that falsifying a government document is grounds for disciplinary action to be brought against you, which could lead to you being removed from all FPS security guard service contracts.

The DHS Form 139 should remain in a secure place designated by FPS. It should never be carried around by any individual or left in an unsecured place.



## 8.2: General Guidelines for Report Writing

Paperwork associated with report writing will not be overwhelming if you:

- carefully read all instructions, including those that might be in the duty book;
- make written and/or mental lists of the required forms and procedures to fill them out;
- ensure you have the required forms on hand, or know where to procure them; and
- practice the gathering information, note taking and reporting techniques that are addressed in this chapter.

## 8.3: Collecting Information for Reports

In responding to an incident or emergency, you will have several possible courses of action depending on the situation and decisions made by FPS law enforcement personnel. You are not required to conduct interviews, however the first of such actions may begin with collecting information. This chapter provides some useful guidelines for gathering the necessary information for your report.

You may be required to obtain information from people connected to an incident or crime. The goal is to gather information that will help FPS law enforcement personnel develop leads, aid in locating property or people, assist in clearing suspects and verifying suspicions. You may help other people give an account of what happened in their own words. You then review their statement, and ask questions if necessary to help clarify any information. Some general points to remember when collecting information are:

- establish your authority to ask questions by properly identifying yourself and stating your reasons for asking questions;
- always politely ask for people's assistance and cooperation;
- make sure your questions are clear and concise so people will understand them;
- maintain your focus, be positive and thorough! do not allow your thoughts to wander;
- have your questions written down to be clear on what you are asking;

- the most commonly asked questions will refer to **who, what, where, when, how** and **why?**; and you will also want to ask if there were any witnesses to the incident.

You must stop asking questions if it becomes apparent that your information gathering has stopped being a general inquiry into the incident and now focuses on the person with whom you are talking. People have the constitutional right to refuse to answer questions that might incriminate them. This also applies when answers provide a link in a chain of evidence that could be incriminatory.

At the conclusion of the discussion, thank the person for his/her cooperation. Report your findings to the appropriate FPS official and file your incident report.

### Obtaining Descriptions

Often witnesses or victims will have trouble giving accurate descriptions of suspects for reasons ranging from their excited emotional state to the swiftness of the incident. To prompt their memories, ask questions that go from general to specific points.

Questions about a suspect's physical characteristics should begin with the head and proceed downward. Take care not to ask questions that will influence the person's response. Rather than asking, "Wasn't the subject six feet tall?" ask "Do you see anyone here about the suspect's height?" Using other points of reference will help the witness recall characteristics that would otherwise be overlooked—including mannerisms, speech and clothing.

Aside from general physical characteristics such as height, weight, sex, age, scars, marks, race, etc., use the following list that may help you to develop a profile of the wanted person:

- **Head**—Size and shape;
- **Hair**—Color, whether straight, curly, wavy, etc.;
- **Ears**—Size and shape;
- **Face**—Shape, facial hair (beard or mustache);
- **Eyebrows**—Arched, straight, long, slanted, etc.;
- **Eyes**—Color, shape, did individuals wear glasses?;
- **Nose**—Size, width, did individual have flaring nostrils?;
- **Mouth**—Size, type of lips;
- **Speech**—Lisp, mumbled, accent, drawl;

- **Voice**—High, low, raspy, loud, soft; and
- **Chin**—profile-receding, jutting, small, pointed.

If known, information on the habits and behavior of the suspect will be extremely helpful.

Question each victim or witness alone, and check the blocks that match his/her description on the appropriate form. Don't put words into the individual's mouth, and don't make a composite description of a suspect by combining various descriptions. Place any additional descriptions in the Remarks section.

## 8.4: Taking Notes

The purpose of notes is to help you do a final written report in response to any call or complaint. Reports begin a chain of events that may include a future review by police, attorneys and judges. They become a permanent record. If you want to write an effective report, it all starts with taking notes. They are the foundation for your actual report. By applying effective note taking, you will write a report with less difficulty and in less time.

Take down the information. Get it all, get it right and make it clear. Then answer the following questions when you are collecting information. This will save you the embarrassment, inconvenience and imposition of having to re-question a victim, witness or complainant.

When taking notes, you should answer the following key questions.

- **Who**—When individuals are first mentioned in a report, give their first, middle and last names. The first time witnesses are introduced, identify them with brief descriptive phrases; give complete descriptions of suspects, prospective defendants and prisoners.
- **What**—Provide just the facts on what happened.
- **When**—This is the date and time the incident occurred, or an approximation of the same. Make sure you write the information down when told, so you have it correctly for your report.
- **Where**—This is a definite place to the exclusion of all other places. It should be so clearly identifiable that no confusion or misinterpretation is possible.
- **Why**—This is particularly significant where intent is an element of the offense. In such cases, give

the facts regarding intent with such clarity that there is no need for your conclusions or opinions.

- **How**—This describes how incidents transpired. You want to be sure and establish the sequence of events as they occurred. Be aware if you have different witnesses, you will probably have different versions of how the incident happened. It is not your job to determine which version may be the correct one, only to record the information as told to you.

In the event you will have to do a report, you will need to make sure you have the following information:

- type of incident or offense;
- date, time and location of same;
- full names and addresses of personnel involved; also include business addresses and telephone numbers;
- DOB, sex, age and race;
- if any injuries, describe them; if any injured are treated, describe the first aid provided; also, annotate anyone who refuses treatment;
- time of notification to the FPS MegaCenter; and
- any notification of additional emergency services, building management, etc., to include names and telephone numbers of those contacted.

Other specific information required for your report will depend on the type/nature of incident or offense. Refer to your post orders.

For any utility emergencies, contact the FPS MegaCenter and log in all applicable information. The FPS MegaCenter will contact the responsible company(s) and report the nature of emergency along with any specific instructions.

The more in-depth your notes are, the easier your report writing becomes. These notes should be so comprehensive that several months later you should be able to refer back to them and have accurate recall.

It is important to remember that Federal Rules of Evidence allow any material used to help you recall information or write reports to be entered into evidence during a trial. Make sure your notes are factual, legible and free of anything that may damage your credibility, that of your co-workers or of any FPS personnel.

These notes when completed contain sensitive information and will not be distributed outside the FPS. You are not allowed to have personal copies or provide anyone else copies unless authorized by competent authority to do so. If you do, you will be subject to possible disciplinary action.

## 8.5: Report Writing

A report relays information and tells a story. It is a clear, concise representation of a crime or incident. The report must be comprehensive and leave out no important information.

Your report when properly submitted on DHS Form 3155 (offense/incident report), is the official record of the incident. Follow the instructions shown on the reverse side of the form, fill in all numbered items applicable to you. Record all items not related to the incident as “not applicable” or “N/A.” If additional space is needed, use the reverse side and continuation sheets. The continuation sheets should be annotated with the case number and date at the top of each sheet. Pages should be numbered at the bottom. Refer to Appendix 2 of this manual for samples of the form.

It is possible in addition to the Form 3155 that you will have to complete a copy of DHS Form 3157 (crime information), which is used to describe the offense and any suspects, victims or witnesses. A separate form is required for any person(s) involved in the aforementioned categories. Upon completion of the form, it will be attached to the Form 3155.

If required to fill out either form, keep the following responsibilities in mind: Consider exactly what it is you are trying to accomplish. You must address those elements that show a crime or incident did occur. The report must contain statements or observations that have a direct relationship to the crime or incident. Observations must be yours—not what another person sees. Your direct information eliminates misleading circumstantial evidence.

One portion of the offense/incident report is a short narrative describing the incident or offense. Although a narrative, it should contain all the pertinent facts and information. It should relay the information just as you received it. To assist you, the following guidelines will be helpful.

- You should have a **plan**—determine the purpose of the report and then prepare an outline with topic headings that distinguish between major and minor sections. This should be started at the note-taking stage, so writing the report will be less time consuming.
- Next you should **organize** your background material in the order detailed in your outline. Put it in the order you will use it in the report.
- Now you are ready to **write**, using directives, official sample reports or copies of other well written, approved reports as guides. Again, be clear and concise, describing just what happened.

After finishing the report, you will need to proof-read it for mistakes and any errors. While doing so, ask yourself the following questions:

- does the report properly communicate what occurred?;
- does it meet the criteria for the investigation?;
- can your supervisors or other superiors make decisions based on the content of it?;
- does it answer the who, what, where, when, why and how?;and
- does any part seem unclear to you?

When doing any reports, always check for inconsistencies, unnecessary repetition, inadvertent omissions of information, etc. If able to do so, set the report aside for a few minutes and then review it a second time.

## 8.6: Filing Reports

When you have completed your report, notify the appropriate FPS official and/or the FPS MegaCenter. The report should be collected and forwarded to the applicable office. The reports become official documents once submitted and approved by an FPS official. If a party has a need for a copy of a report, you will direct them to contact the responsible FPS office. You are never under any circumstances allowed to make copies, keep copies or release copies of any reports you have written.

You should also be aware that any reports done by you not meeting all the FPS criteria will be re-written.



# Chapter 9

## Special Situations



Over time, you will be exposed to a variety of unusual and sometimes dangerous situations that will tax your ingenuity and ability as a security guard. Usually you will not be working alone in special situations. In most cases, highly trained specialists and/or law enforcement personnel must be called. However, you too could be crucially important because of your early arrival on the scene, knowledge of the building and its occupants and the ability to quickly summon any needed assistance.

### 9.1: Escort Duties

FPS does not normally require security guards to provide escort duties. There are rare occasions however when this may be a requirement. If required to escort someone from one location to another, apply the following:

- follow the person at an approximate distance of 4-5 paces;
- never allow another individual to move between you and the person being escorted; and
- do not be distracted and/or lose sight of the person being escorted.

Escort duties are authorized only if contained in your post orders or you receive approval from the FPS MegaCenter or your supervisor. You will notify your supervisor and the FPS MegaCenter at the beginning of and upon completion of the escort detail. These duties cannot be performed for non-government agencies/personnel and you are not allowed to go off government-owned/controlled property.

If you observe an incident such as a robbery or assault while performing an escort, you are not allowed to intervene. You will remain focused on

your escort duties and contact your supervisor and/or the FPS MegaCenter relaying the information and following instructions given to you.

### 9.2: Dealing with Seriously Disruptive Behavior

Because government buildings are open to the public, they will often attract vagrants prohibited from entering private buildings. This will occur mainly during inclement weather and during the cold weather season. Some of these people may display erratic, seriously disruptive behavior.

The possibility also exists that you will come into contact with someone that is upset for various reasons with the government or a government employee. He/she will intentionally enter the facility and cause serious disruption to the normal flow of business.

In either instance, you need to know how to respond. You will **always exercise extreme caution** and never rush blindly into a situation. Properly evaluate the situation to determine the proper course of action. If able to do so, contact the FPS MegaCenter and report the situation, and they will dispatch law enforcement personnel to assist you. Attempt to isolate the individual from other personnel and do not allow a crowd of onlookers to form. This will sometimes only tend to agitate the individual.

If it becomes necessary for you to use physical restraint before law enforcement assistance arrives, use only the minimum amount of force necessary to contain the situation and contact the FPS MegaCenter to provide them a situation update.

### 9.3: Code Adam

Code Adam, one of the country's largest child-safety programs, was created and named in the memory of 6-year old Adam Walsh, whose abduction from a Florida shopping mall and subsequent murder in 1981 brought the horror of child abduction to national attention. On April 23, 2003 the "Code Adam Act of 2003" became law. It requires that the designated authority for a public building establish procedures for a missing child in a federal facility. FPS implemented the policy nationwide and established procedures for locating a missing child in federal facilities.

If you are approached by a building tenant or visitor about a missing child, the first step is to quickly obtain a detailed description of the missing child. Be sure to get the child's name, age, gender, race, weight, height, hair color and eye color. Also, it is very important to include the clothing the child was last seen wearing including shoes. An abductor may change how a child is dressed by adding or removing a jacket or sweatshirt, but the shoes will often stay the same.

Once you have a complete description, contact the FPS MegaCenter. Be sure to provide the operator/dispatcher with the complete description. The FPS MegaCenter will notify FPS law enforcement personnel and security guards, as well as any other law enforcement entity. Be certain to comply with any instruction issued by the FPS MegaCenter or FPS law enforcement personnel.

It is important for you to maintain a heightened state of awareness. Monitor all access/egress points for a child that matches the description. If so directed by FPS personnel, you may be required to search the interior of the building, as well as any exterior areas on the property. You must search all rooms—locked and unlocked, restrooms, storage areas and any potential hiding places.

If you see someone with a child that matches the description, immediately detain them and contact the FPS MegaCenter. If you are unable to detain them, notify the FPS

MegaCenter and describe the person accompanying the child. If you locate the child, immediately notify the FPS MegaCenter, and they will decide how best to reunite the child with a parent or guardian and cancel the "Code Adam" alert.

# Chapter 10

## Emergency First Aid



Each day, countless medical emergencies, from the relatively minor to the most critical, occur in government buildings. The most important thing to do in a medical emergency is to contact the FPS MegaCenter and report the incident. However, if you are alone and the victim is seriously injured, your primary task is to apply emergency first aid. Your quick action could save a life.

### 10.1: First Aid/CPR/AED

First Aid, Cardiopulmonary Resuscitation (CPR) and the Automatic External Defibrillator (AED), are all critical techniques/equipment to assist you in your preliminary medical assistance endeavors if/when necessary for injured personnel and/or to maintain life when a person's breathing and heart functions may stop.

As part of your training, and before you begin work as a FPS security guard, you will be instructed and then certified in First Aid, CPR and on the AED. Your training will consist of techniques used by the American Heart Association and the American Red Cross. Once the training/certification has been completed, you will receive a certification card, which will have an expiration date on it. All of the above training requires re-certification as shown:

- **First Aid**—every 3 years; and
- **CPR and AED**—annually or when the current certification expires.

It is the responsibility of your employer and yourself to ensure you receive the re-certification training. You should notify your supervisor and employer a minimum of 60 days prior to your expiration date and again at 30 days prior if you have not been con-

tacted. **You will not be able to work on any FPS security contract if any of your certifications are expired.** If you are found to be in possession of an expired card by FPS, you will be removed from the contract until renewal.

If while on duty you receive a request for emergency medical assistance or observe someone needing assistance, remain calm and apply the techniques you learned in your training. If it is determined emergency medical services are required, telephone them immediately and do what you can until they arrive. If able to do so, contact the FPS MegaCenter first and relay the situation to them. The operator/dispatcher will assist you in any way he/she can.

### 10.2: Blood Borne Pathogens

As a security guard and a first responder to incidents, you could possibly face exposure to infection. Blood borne pathogens are disease-causing microorganisms that are present in the blood, human blood components and products made of human blood. In providing emergency first aid, you may be exposed to blood borne pathogens contained in the blood and/or body fluids of the victim. The Human Immunodeficiency Virus (HIV) and Hepatitis B (HBV), are blood borne pathogens. The primary way to transmit HIV or HBV is through blood-to-blood contact. If in a situation involving blood, the following precautions are recommended:

- avoid contact with any body fluids;
- wear protective clothing such as disposable gloves to cover any cuts, scratches, or skin conditions;
- wash your hands immediately with soap and water when done even if you wore gloves;

- do not eat, drink, smoke or chew gum when giving first aid;
- do not touch your mouth, nose or eyes when giving first aid;
- do not touch any objects soiled with blood;
- avoid handling any sharp objects if possible such as knives or needles;
- use a CPR mask if one is available; and
- always follow the approved instructions for handling and disposing of any items with blood and/or bodily fluids.

If you think you have been contaminated while performing emergency medical assistance, isolate yourself and contact your supervisor and/or the FPS MegaCenter immediately.

# Chapter 11

## Combating Terrorism

The USS Cole, the U.S. embassies in Africa, Flight 103 over Scotland, the Alfred P. Murrah Federal Building in Oklahoma City and the Twin Towers in New York were all targets of terrorism. Major acts of terrorism against United States property and citizens are a real-time, ever present threat. Federal property represents a particularly attractive target for terrorists. You will play an important role in deterring acts of terrorism against federal facilities and as a forceful respondent to a terrorist attack against your facility should one occur.

### 11.1: What is Terrorism and Who Are Terrorists

Terrorism is the calculated use of force, violence or threat of violence against persons or property to achieve a political or religious goal. These goals are achieved through intimidation, coercion, fear or by seeking ransom. Terrorism is directed against governments, businesses, communities and individuals. It may be done to retaliate for perceived injustices; to cause a confrontation between parties; to improve a bargaining position; or to demonstrate strength, commitment and resolve. Terrorism is intended to convince the public that their government is powerless to prevent terrorism and to get publicity for the terrorists' cause. The probability of a terrorist act occurring is statistically low, but when an attack does occur, it usually has a major local, regional, national or even global impact. Terrorism is a threat during peacetime and war. All acts of terrorism are crimes punishable under Title 18 USC. Terrorism in the U.S. is categorized by the FBI as either **domestic** or **international**. According to the FBI, the U.S. has been the target of over 32 percent of all terrorist attacks worldwide, second only to Israel.



**Domestic terrorism** involves groups or individuals without foreign direction whose activities are directed at elements of our government or our population. In the U.S. there are a number of paramilitary and terrorist groups whose objectives include animal rights, conservation and ecology, anti-law enforcement, race supremacy, anti-taxation and overthrow of the government.

**International terrorism** involves groups or individuals whose activities are foreign based and directed by countries or groups outside the U.S. They tend to be religious or ethnic organizations that have major grievances with the U.S. The Department of State considers seven countries (Libya, Syria, Iran, Cuba, Sudan, Iraq and North Korea) to be sponsors of international terrorist groups.

Some terrorist groups are evolving into new organizational structures that are harder to detect and infiltrate. These terrorist groups form, change and regroup in response to specific agendas or planned actions. Terrorists almost always act with a specific objective in mind. They are very dedicated and willing to make great sacrifices to be successful. Generally they are well trained, often with a military or paramilitary background. Many groups are also well funded and well equipped. They conduct surveillance activities to gather information on potential targets, sometimes for weeks or months before acting. Not only do terrorists plan their attacks in great detail, they also rehearse their operations.

Terrorists want media coverage to ensure that many people know about their activities. That is why they select high-visibility targets and attempt to do maximum damage. Terrorists hope that the attention will increase the public's fear, cause a planned government reaction or attract sympathy to their cause.

Many terrorists are willing to die for their beliefs, and this factor alone makes them extremely dangerous.

## 11.2: Types of Terrorist Attacks

There are seven basic types of attacks that terrorist groups will use. They are hijacking, kidnapping, bombing, assassination, armed assault, hostage taking and using nuclear, biological or chemical (NBC) weapons, also referred to as Weapons of Mass Destruction. During their operations they will use handguns, automatic weapons, explosives and now Weapons of Mass Destruction.

A terrorist group's objectives and capabilities dictate which types of attack it will employ. Most terrorist incidents in the U.S. have been bombing attacks. These have involved explosive devices ranging in size from letter bombs to truck bombs. Bombings generally provide the greatest damage and publicity at the lowest risk although other types of attacks have been used. At federal facilities, a bombing/WMD attack is the most likely threat, followed by armed assault, assassination and hostage-taking.

The effects of terrorism can be devastating and include psychological trauma, physical injuries, loss of life, property damage and major disruptions in utility, water, transportation and communications services.

## 11.3: Weapons of Mass Destruction (WMD)

One morning in March 1995, the Japanese cult group Aum Shinrikyo committed a terrorist attack in the Tokyo subway system during rush hour. Cult members placed canisters containing sarin, a nerve gas, into five separate subway cars on three different subway lines. As the gas spread throughout the trains, thousands of people were overcome by the toxic effects. The attack killed 12 people and injured more than 5,000 others. The incident stunned the world, for it was the most publicized terrorist attack based on the use of a chemical agent.

There are many experts on terrorism who believe the WMD attacks will become the preferred means of terrorist attacks in the future. Chemical and biological agents such as sarin, anthrax, botulism toxin and VX gas are relatively inexpensive to make or obtain and can cause mass casualties. Chemical and

biological weapons are particularly dangerous for three reasons:

- they do not necessarily take effect immediately;
- they may be invisible to the human eye; and
- they may not have a scent.

In a chemical or biological agent attack, large numbers of people can be afflicted or overcome before anyone can determine what has happened, what the agent is, where it is placed and when it was released. Even tiny amounts of some chemical or biological agents can be lethal.

For the above mentioned reasons, you should be aware of what you can do to help prevent and how to respond to possible terrorist incidents involving WMDs.

## 11.4: Preventing Terrorist Attacks

As a FPS security guard, your best countermeasure in preventing a possible terrorist attack against the facility you are protecting is to be vigilant in performing your assigned security duties. A first impression carries a lot of weight. A terrorist would normally prefer a "soft" target, meaning there essentially are no security measures in place. However, if they are able to see a security guard that's attentive, sharp, alert and professional, your facility in their mindset would be a "hard" target to them, and they would probably seek another target.

To succeed in their mission, terrorist operations require detailed information for planning and executing an attack. Terrorist organizations may be provided information on the target and the environment by entities sponsoring them or they may collect it on their own.

Because of good intelligence collection and detailed planning, terrorist attacks are often successful. It is during the phase of their information collecting and planning that you can be helpful. By being alert and observant, you may notice something out of the ordinary or strange. Since you should be familiar with your facility and the surrounding environment, this would be easy for you to do.

During the performance of your duties, anything appearing out of place should be investigated. If your post is the rover, randomly change your

security checks and routes for your assigned area. You have the authority to challenge people taking part in an action you determine to be suspect. In any case, you should immediately report any activities you are suspicious of to your supervisor and the FPS MegaCenter.

As mentioned earlier, your powers of observation and the ability to notice something out of the ordinary will be assisted by your familiarization with the facility. Knowing normally what people are in what area, any illegally parked/and or unmanned vehicles, a backpack or suitcase left unattended, people appearing to be bystanders but focusing too much on the building are all examples of what might possibly be out of the ordinary for day-to-day operations at your facility. Only you would know!

### **11.5: Responding to a Terrorist Attack**

Your response to a terrorist situation will be similar to those of other emergencies. Your job remains to protect life and property, to assist injured personnel, to secure the area and protect any evidence and to assist the responding law enforcement and life/safety personnel as required. These are accomplished by:

- knowing your post orders;
- being familiar with the OEP for the facility;
- knowing of any secure and/or restricted areas within the facility;
- knowing all of the main access/egress points; and
- being familiar with the facilities security alarm and CCTV systems.

In the event of a terrorist attack, the FBI will assume jurisdiction and coordinate the federal response efforts. You will more than likely be directed by the FPS MegaCenter to provide them assistance. Your attention to detail will be very helpful in this type of incident. You could possibly provide valuable information such as descriptions of the personnel involved, vehicle information (types/number involved), events leading up to the attack, did the CCTV system record anything and any other specific information you may be able to offer. You should write all applicable information down while it is fresh in you mind and provide a written incident report as soon as possible. Make sure you keep the FPS MegaCenter and your supervisor informed.

Page 58  
Left Blank Intentionally



# Chapter 12

## Workplace Violence

Violence is becoming more common in our society. Violent acts are occurring more frequently in our places of work to include government facilities. As a security guard, it is your job to help keep violent acts from occurring and, should prevention fail, respond promptly and effectively to protect threatened individuals and restore order.

### 12.1: What is Workplace Violence

We are living in a society more violent now than in the past several generations. More people deal with their problems through violence. Much of this violence spills into the workplace. Workplace violence can be by anyone against anyone else in the working environment. The definition of workplace violence is not intended to replace the legal definition of assault or other crimes of violence. It is simply the commission of violent crimes at a place of work.

There are multiple terms used to describe various aspects of workplace violence. Most people agree that physical force against a worker is an example of violence. But violence can take many other forms. These can include non-physical forms like verbal and non-verbal incidents, threatening statements, gestures and persistent personal harassment. Physical injury is not the only result of workplace violence. Personnel may suffer from long-term psychological trauma, although it may not be recognized immediately.

### 12.2: Who Commits Violent Acts and Why

Workplace violence is not limited to a specific person or group of people. The potential exist for every workplace. Conventional wisdom, often

perpetrated by the media, has it that people “snap” one day and commit acts of workplace violence just “out of the blue.”

However, that may not usually be the case. In many cases, an act of workplace violence is the result of an observable pattern of increasingly violent behavior over a period of time. The following is a series of steps that can signal potentially violent acts:

- discontentment;
- nonspecific verbal intimidation;
- nonspecific verbal threats;
- written threats;
- specific verbal threats;
- physical violence against property;
- physical violence against people without the use of weapons; and/or
- physical violence against people with the use of weapons.

An individual’s actions can move across the scale and his/her behavior can escalate or de-escalate over a period of days, weeks or months. Generally, the behavior becomes increasingly more violent. The entire process can occur within a period as short as one week or as long as one year. The outcome would depend on the circumstances. When an individual comes to believe that violence is the only solution to his/her problems, the results can be catastrophic.

People who have engaged in acts of workplace violence have reported afterwards that if someone had been able to listen, understand and work with them, they would not have acted violently.



### 12.3: Preventing Workplace Violence

If you know the signs of violence in the workplace, you can predict them and in many cases prevent them from happening. There are various ways that you can help to reduce or eliminate the chances of violence in your facility:

- know and recognize employees who have been laid-off or fired; their access into the facility may be restricted;
- knowledge of and adhering to your post orders; they were written to prevent crime and maintain order within your facility;
- maintain a visible and professional appearance; your presence and awareness is enough sometimes to deter a violent act;
- be aware of the environment; you will probably have knowledge of any type of disputes, disagreements ongoing possibly between the management and employees; and
- be aware of any incidents of verbal abuse, threats, intimidating tactics or any other potential situations that could escalate into violence; all of these should be reported to the FPS MegaCenter immediately and a written report done.

- in the event you have to detain an individual until law enforcement personnel arrive, you will use only the minimum amount of force necessary. You should be guided by your judgment and training.

**The use of deadly force is authorized only to save the life of yourself or others.**

### 12.4: Responding to Incidents of Workplace Violence

Your duty book and/or post orders will provide specific procedures for responding to violent incidents in the workplace, which should be similar to the steps below:

- if you observe a violent incident developing or occurring, and it is safe to do so before acting, immediately contact your supervisor and the FPS MegaCenter;
- if the situation warrants you to act first to protect yourself and/or other personnel from imminent danger, take the appropriate action and when the situation is under control and contained, then make the necessary notifications;
- if possible, attempt to verbally defuse the situation by separating the parties that are involved; do not allow co-workers to engage in the situation;

# Chapter 13

## Civil Disturbances



In the United States, the right of lawful assembly is protected under the First Amendment of the Bill of Rights. Every state in the Union, by its Constitution, similarly protects this right. The purpose of this chapter is to give you some knowledge of crowd behavior and to discuss procedures for handling people at public events, parades, fires, traffic accidents and minor disturbances.

### 13.1: Types of Civil Disturbances

A **crowd** is a large number of people collected into a close body without order. Although innocent in its origin, nature or purpose, a crowd can evolve into a mob. This mob in turn, can degenerate into an unlawful assembly or riot (i.e., a civil disturbance). There are two major categories of crowds; **casual** and **psychological**.

A **casual** crowd is an assembly of people showing no group behavior but merely denseness of contact. Examples of this type of crowd are shoppers at malls or people waiting at the airport.

A **psychological** crowd is an assembly of people who have a common interest or respond emotionally to the same stimuli. Examples of this type of crowd are people at ball games, concerts, political speeches, parades and fires.

There are four types of psychological crowds: **friendly**, **sightseeing**, **agitated** and **hostile**.

- A **friendly crowd** is the type that is well behaved and requires only the simplest control by security personnel. However, this type of crowd can become a problem from improper handling. Examples are ball games, church meetings and parades.

- A **sightseeing crowd** is people who gather together at the scene of an accident, fire or disaster. This type of crowd is curious, cooperative and anxious to assist. But it can become overzealous and a liability to security guards and FPS law enforcement personnel. Examples are crowds that interfere with rescue operations, destroy evidence and place themselves in danger.
- An **agitated crowd** is a friendly or sightseer crowd, which becomes disturbed by emotional influences or swayed by irresponsible parties. An example would be an accident scene where an ambulance does not arrive promptly and the crowd becomes angry at the authorities for their lack of responsiveness.
- A **hostile crowd** is one that is willing to be led into lawlessness, but it lacks the courage and unity of purpose. An example of this is a civil disturbance brought on by a mob or riot.

### 13.2: Impacts of Civil Disturbances

Every crowd should be viewed as a possible security problem. Friendly and sightseeing crowds can become agitated with improper handling or lack of perceived action on the part of security/law enforcement and life/safety personnel. However, planning for these types of crowd reactions is difficult, so the use of your best judgment becomes very important.

A crowd at a public incident or disturbance is the most difficult type to control and can turn into a hostile crowd. This type of crowd leads to a civil disturbance by turning into a mob or a riot. A **mob** is when a crowd becomes excited or its members lose respect for law and order and follow its leaders into mass lawlessness. A crowd will deteriorate into

a mob if it has been preconditioned by irritating events and rumors, and it has been inflamed by agitators appealing to emotion rather than reason. A mob turns into a **riot** when its actions supplant lawful control, law and order disappears, and anarchy results.

A mob or riot does not need to be planned in order for it to occur, nor may it result from deliberate intentions. In a mob or riot situation, actions that ordinarily would be regarded as extreme are now considered acceptable within the group. This is because typical law-abiding citizens allow themselves to lose all self-control and obey the “law of the pack.”

### 13.3: Demonstrations

The nonviolent demonstration has become widely used in the last two decades to protest social, economic or political conditions.

**Demonstrations** are different from crowds and mobs in that they are organized, have leadership and have members who are nonviolent and disciplined.

You must protect peaceful demonstrators who are exercising their constitutional right to demonstrate, and you must protect the general public from those who infringe on the rights of others. The most common problems occur when demonstrators decide to engage in sit-ins and incidents that violate the property rights of others.

Demonstrations can be infiltrated by people who have a violent or undisciplined agenda. This happened in Seattle, Washington in 1999 during a demonstration protesting a meeting of the World Trade Organization (WTO). They successfully infiltrated the demonstration and it quickly exploded from a peaceful event into an unlawful mob/riot situation.

This means you, as a FPS security guard should always be alert for violent elements in an otherwise peaceful demonstration realizing it could turn into a mob or riot situation in a short period of time with little warning.

### 13.4: Response Procedures

Decisive control measures are necessary when you are dealing with civil disturbances, demonstrations or crowds. These control measures must be employed quickly and with confidence. These measures must be effective so that life and property as well as the principles and security of law and order will not be jeopardized.

Crowds cannot be controlled without sufficient manpower. If a crowd develops in your vicinity and it appears that it is not going to disperse quickly, call the FPS MegaCenter to report the situation. In most cases, FPS law enforcement personnel or local law enforcement personnel will be dispatched immediately to your location. Should you have to act before assistance arrives, remain professional and firm. Do not allow yourself to lose your temper and forget your bearing. **You never use unnecessary or excessive force, you never threaten someone or use derogatory language/gestures** when attempting to defuse a situation. The aforementioned will only serve to incite a crowd to aggressive hostility and compound the violence. Potentially dangerous crowds can usually be controlled by the following:

- removing or isolating individuals involved in the incident before the crowd can unite;
- breaking the crowd into small, isolated groups;
- removing or isolating the leaders; and/or
- diverting the attention of the crowd.

Whether you realize it or not, you being in top-notch physical condition also enables you to perform better in these types of situations. You may be required to work long hours, you may have to respond physically, you need to be mentally alert, and be able to handle the stress and fatigue. Proper physical conditioning will assist you in accomplishing your mission.

# Chapter 14

## Bombs/Weapons of Mass Destruction (WMD) Threats and Incidents



Bombings or the threat of being bombed or attacked by Weapons of Mass Destruction (WMD) are harsh realities in today's world. The public is becoming more aware of incidents involving the use of explosives and WMD. The USS Cole, the World Trade Center and the Alfred P. Murrah Federal Building are all stunning examples of what can happen. Although you may not be aware of the fact, bomb threats occur on a daily basis nationwide.

Although they are still uncommon, law enforcement agencies take acts or threats involving the use of WMD very seriously. Most agencies to include the FBI, have provided regular intra-agency and inter-agency training to their employees on WMD threats and responses.

As a FPS security guard, your responsibilities in responding to these threats are to reduce the possibility of injuries to personnel, damage to property and disruption of operations.

### 14.1: Receiving Bomb/WMD Threats

Bomb/WMD threats are received in a variety of ways, the majority being called in directly to the intended target(s). They may however, be received in writing or on a tape. On occasion they will use a third party such as a newspaper or television station, all intended to gain them more publicity. When these threats are received by whatever means, the proper authorities (local police, the FBI) are contacted immediately.

There are two logical explanations for warning of a bomb/WMD incident. In some cases, the caller has knowledge of an explosive or incendiary device that has been put into place, either having placed it there or finding out by some other means. In the scenario, he/she wants to minimize personal injury and/or property damage. The other explanation is

the caller wants to create an atmosphere of panic and chaos causing disruption of normal operations.

You must take any/all bomb or WMD threats you receive very serious. You will attempt to obtain as much information as possible from the caller. It is not your responsibility to ascertain if it is real or a hoax. If possible, alert another guard to contact the FPS MegaCenter while you are still on the line with the individual, without alerting him/her to your actions. Procedures for handling bomb/WMD threats should be outlined in your Post Orders. You should take the following steps:

- record the date and time of the call;
- attempt to record the exact words of the caller;
- pay attention to/for any background noises;
- listen to the caller's voice for any identifying aspects such as sex, possible age, if the voice is monotone or excited, if he/she appears upset or has any noticeable speech impediments, etc.;
- remember to **try to keep the caller on the line**, and do not hang up; by now, the FPS MegaCenter will have been alerted and be acting on the situation.

There are specific questions listed below you should ask the caller:

- when is the bomb/device going to explode?;
- where is it right now?;
- what does it look like?;
- what kind of bomb/agent is it?;
- what will cause it to explode?;
- did you place the bomb/agent?;
- why?;
- what is your address?; and
- what is your name?

If you receive a written or recorded threat, save all the materials, including any envelopes or containers associated with the received threat. Once you recognize the message as being a bomb threat, cease handling the material. Maintaining any evidence such as fingerprints, handwriting, postal marks or the paper is extremely important.

If someone else reports having received a bomb threat to you, alert the FPS MegaCenter and your supervisor immediately. A guard will be dispatched to that location to take a report from the individual immediately while the information may be fresh in his/her mind. Use the questions listed above as your question guidelines. You should remain calm and professional. If the individual is excited or scared, attempt to calm them down so you can get details as accurately as possible. (Refer to the sample questionnaire form contained in Appendix #2 of this manual).

## 14.2: Reporting Bomb/WMD Threats

You will immediately report any bomb or WMD threat received by any means to the FPS MegaCenter and your supervisor. It is not your responsibility to determine if it is a credible threat or not. When reporting the threat, avoid using your radio or a cellular phone for the following reasons:

- the radio waves or cell phone frequency might trigger a detonation; and
- you don't want to cause panic and confusion by someone overhearing your call.

Unless directed by your post orders or the emergency plans in your duty book, the FPS MegaCenter will make all appropriate notifications. Once you have made the report and provided all information available to you, remain on post and await further instructions.

## 14.3: Locating and Handling Suspicious Items

A suspicious item is one that does not fit its surroundings; it looks or seems out of place, you may have never noticed it at a particular location before or it just doesn't seem to belong there at a certain time. Most bombs are homemade; their designs and

methods of concealment are limited only by the imagination and resources of the builder. Bombs can be constructed to look like almost anything and can be placed or delivered in any number of ways. The probability of a bomb looking like a bomb is relatively low, since bombs are usually concealed in packages, briefcases, gym bags, luggage, boxes or other containers. In some cases the bombs or their containers may have odd markings, make sounds or have a distinctive odor. If you encounter objects that have a strange odor, such as the smell of almonds or petroleum products or if you encounter any type of suspicious looking liquid or gaseous substance in a container, **do not touch or open it**. Immediately report the object(s) to the FPS MegaCenter.

It is quite likely you may come into contact with a suspicious object/package while performing your duties as the rover, at an access/egress point or while operating the x-ray machine. Some of the signs to look for are excessive postage, an incomplete address, oil stains on the wrapper, unusual smells and distorted handwriting. If you suspect there may be a bomb at your location, clear the area of all personnel.

In certain situations, when a bomb threat is received, you may be required to assist in a search of the facility. If your facility has a bomb threat plan, make sure you review it. Remember you are looking for something unusual or out of place. Some additional guidelines are:

- turn off your radio (the frequency could act as a detonator);
- allow no unauthorized people to enter the area;
- when checking the exterior, search bushes, window ledges, flowerpots, benches, garbage cans and air conditioning units;
- when entering an interior space, stop and listen for any sounds and smell the air for any unusual odors; and
- upon checking an interior room, use the four level method: (first is search waist high to the floor, second is search waist high to the top of your head, third is search from top of your head to the ceiling and fourth is search above the ceiling).

## 14.4: Response Procedures

If FPS makes the determination a bomb or WMD threat is credible, they will notify the designated official for the facility and initiate the emergency evacuation plan in conjunction. You should be familiar with the emergency evacuation plan and be prepared to perform your specifically assigned duties according to the plan, which will be contained in your duty book.

You will not discuss the situation with any outsiders or any media personnel. All inquiries from the media will be directed to the FPS MegaCenter if the facility does not have a designated spokesperson.

If an explosion occurs, or you note the smell or see a substance dissipating from an object, sound the alert immediately. Contact the FPS MegaCenter and your supervisor and follow procedures as outlined in your post orders/duty book. It is imperative you maintain your composure, your professionalism, and remember your training during a stressful time like this.

Page 66  
Left Blank Intentionally



# Chapter 15

## Hostage Situations



One of the most difficult situations that you may ever have to deal with is a hostage situation. Such a situation may result from a terrorist attack, a bungled robbery, a domestic dispute or a mental breakdown. You may personally observe the incident or be called upon to respond. You may be the first one on the scene or be a part of the response force. In any event, you must know what to do and how to do it; lives will be at stake.

### 15.1: What Is a Hostage Situation

In a hostage situation, at least one person is being held against his or her will by one or more subjects who may threaten to harm the hostage(s). The subject usually has weapons or explosives. The subject will usually take over a room or a building. The subject usually wants to negotiate release of the hostage(s) for a set of conditions, but this is not always the case. Once a situation has escalated to the point where hostages have been taken, the likelihood for logical behavior by the subject is greatly reduced.

### 15.2: Reacting to Hostage Situations

If you become aware of a hostage situation, you will immediately notify the FPS MegaCenter and your supervisor. If possible, position yourself where you can see the subject(s) and/or the entrance to the area where he or she is located. Use cover to protect yourself and direct any bystanders to safe positions behind cover or out of the area, if possible.

Attempt to control access to the area. Do not let anyone in except law enforcement personnel. Try to learn from bystanders how many subjects there are, how they are armed and how many hostages are with them. If they can provide you with descrip-

tions of the subjects and/or hostages, or information on any who might be injured, it will be extremely helpful. This information will be passed to the FPS MegaCenter as soon as possible.

Some other key points to remember are:

- remain in contact with the FPS MegaCenter, updating them on the situation;
- provide situation briefs to responding law enforcement personnel and follow their instructions;
- do not attempt to contact the subject—you are not a trained hostage negotiator; if the subject should contact you prior to law enforcement personnel arriving on the scene, you do not make any promises, offers or threats; indicate to the subject(s) you have heard the demands and that someone is responding who is able to deal with him or her; immediately pass this information to the FPS MegaCenter;
- maintain observation of the immediate and surrounding area;
- do not discuss the situation with any unauthorized personnel or the news media; and
- remain calm, remember your training and follow your established procedures outlined in the post orders.

**Under no circumstances will you remove your weapon from its holster and discharge the weapon unless you have been given authorization by FPS law enforcement personnel or you are in a situation where the rules of “Deadly Force” are applicable.**

Page 68  
Left Blank Intentionally

# Chapter 16

## Sabotage and Espionage

You must always be alert for and aware of any threats or activities directed against the U.S. government. These activities can take many forms and can be directed against government personnel, operations, equipment and facilities. The threat to our government from foreign and domestic enemies is a very real one and cannot be taken lightly. An important part of your job is to prevent, detect and report any attempts to damage or destroy government facilities, equipment and property. This also applies to any attempt to harm individuals, or steal sensitive government information. To do this, you must be aware of the threats posed by sabotage and espionage.

### 16.1: What are Sabotage and Espionage

**Sabotage** is any activity that interferes with or obstructs the workings of the U.S. government. People commit sabotage by willfully injuring, destroying or attempting to injure or destroy any government facility. Sabotage must be committed with the intent to harm. There are three categories of sabotage: **incendiary**, **explosive** and **mechanical**. Incendiary sabotage occurs when fire is used to destroy government resources. Explosive sabotage occurs when bombs are used to destroy government resources. Mechanical sabotage occurs when equipment in a government facility is destroyed through use of abrasives, contaminants, removal of parts, etc.

**Espionage** is the act of illegally obtaining classified U.S. national security information for use by a foreign government. Despite its tremendous damage, classic spying on behalf of a foreign country is a relatively rare crime. Many experts think that only a small percentage of espionage activities have been detected by the authorities. Money is the leading motive for espionage; however, other motives are

ideology, revenge, coercion and thrills. In almost all cases, espionage is committed by people who have authorized access to classified information and sensitive facilities; not by outsiders who sneak into or break into offices and photograph classified documents. It is very difficult to identify who is committing espionage; the best chance to do so is through your vigilance.

### 16.2: Deterrence, Prevention and Response to Incidents

The deterrence, prevention and detection of sabotage and/or espionage is a difficult task. Just as specially trained counter-intelligence agents of the FBI or military intelligence personnel educate themselves and learn to recognize the “warning” signs, so should you. When you think of your facility and your day-to-day duties regarding access control, fire procedures, bomb threats, sensitive/classified areas, being on the alert for suspicious activity or personnel, all of these contribute to those “warning” signs for potential sabotage and espionage attempts.

Sabotage is most likely to occur during times of international tension or conflict between the U.S. and other countries. This would be the ideal time for a foreign entity to attempt to disrupt U.S. government operations or affect the morale of the people. Recognize that sabotage could be accomplished through state-sponsored terrorism. (For example, if the sponsors were Iraq or Iran).

Espionage is difficult to detect because anyone is capable of committing this crime. It will however, more than likely be someone who has access to classified information or to sensitive/restricted areas. Over the past few years, there have been U.S.



personnel caught, tried and convicted for this very crime. To assist in deterring and preventing possible espionage activities, you can be alert for:

- unauthorized personnel trying to gain entry into restricted areas;
- personnel not in possession of the proper identification/credentials;
- personnel entering office spaces/areas not associated with their duties; and/or
- after-hours activity in classified/restricted areas.

You should be attentive especially after hours and on weekends to personnel known to work with/around classified material. Take note of the belongings they bring into and take out of the building. Watch for signs of nervousness, unease and impatience from them. In the event you observe anything suspicious or notice any personnel acting out of the ordinary or suspicious, contact the FPS MegaCenter and pass the information to them.

You should also be aware that as a FPS security guard, you could be a target for possible recruitment. This has happened to security personnel in the past. Agents for foreign entities are well aware of your role in protecting our federal facilities. They are aware you may have access to secure areas and/or information. They are aware in some cases you control access/egress procedures for the facility. They will use a variety of means to attempt to recruit you, such as money, female companions, luxuries and eventually blackmail if you find yourself in that position. If you suspect you have been approached by a foreign agent, you will notify the FPS MegaCenter and your supervisor immediately for instructions on how to proceed in this matter.

# Chapter 17

## Child Care Centers



Some of the most emotionally devastating television coverage of the Federal Building bombing in Oklahoma City was the different scenes of injured children as they were removed from the debris. Since many federal facilities now include child care centers, this chapter provides some brief information of interest.

### 17.1: Child Care Centers in Federal Buildings

Child care centers operate in federally-controlled space often at or near the federal facility so employees will have easy access to this type of service. This reduces the stress on employees because they know child care will be available, because it is close by and they are able to readily check on their children or respond in case of an emergency.

Child care centers must meet certain standards in order to be licensed to operate. These standards include health, safety and security requirements. Owners and center employees must ensure these standards are continuous and upheld daily.

### 17.2: Your Responsibilities

Security guard responsibilities for child care centers where applicable, will be contained in your post orders and/or duty book. You should be familiar with these procedures. The following list contains some general guidelines to follow if your facility has a child care center:

- become familiar with the center's managers, employees and parents; this will enable you to identify possible unauthorized personnel;

- be alert for any special instructions for restricted access of a parent/guardian; this could exist because of a custody dispute; if faced with a custody situation, follow the special instructions that apply and contact the FPS MegaCenter and your supervisor immediately; the safety of the child is your responsibility.
- visit the child care center occasionally to become familiar with the layout and to have some idea how many children are housed within on a daily basis along with their ages and
- learning the names of the parents and children will prove to be helpful in the event of an emergency.

While visiting the center and greeting the parents/children, never do anything that might be misinterpreted by someone as being physically or sexually abusive, or unprofessional. A complaint alleging any misconduct will have to be investigated. Any indiscretion on your part can subject you to disciplinary action. Should you observe possible abuse of any children, any signs of neglect, potential safety hazards or any suspicious personnel, you will immediately notify the FPS MegaCenter and your supervisor.

A helpless, little child is one of the most precious assets you are charged to protect. You must not fail.

Page 72  
Left Blank Intentionally

# Appendix 1

## Regulations Affecting Federal Property



### **Title 41—Public Contracts and Property Management; Chapter 102—Federal Management Regulation; Part 102-74 Facility Management; Subpart C—Conduct on Federal Property**

#### **Sec. 102-74.365 Applicability**

The rules in this subpart apply to all property under the authority of the General Services Administration (GSA) and to all persons entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations.

#### **Sec. 102-74.370 Inspection**

Federal agencies may, at their discretion, inspect packages, briefcases and other containers in the immediate possession of visitors, employees or other persons arriving on, working at, visiting or departing from federal property. Federal agencies may conduct a full search of a person and the vehicle the person is driving or occupying upon his or her arrest.

#### **Sec. 102-74.375 Admission to Property**

Federal agencies must:

- (a) Close property to the public during other than normal working hours. In those instances where a federal agency has approved the after-normal working hours use of buildings or portions thereof for activities authorized by subpart D of this part, federal agencies must not close the property (or affected portions thereof) to the public.

- (b) Close property to the public during working hours only when situations require this action to ensure the orderly conduct of government business. The designated official under the OEP may make such decision only after consultation with the buildings manager and the highest ranking representative of the law enforcement organization responsible for protection of the property or the area.
- (c) Ensure, when property or a portion thereof is closed to the public, that admission to the property, or the affected portion, is restricted to authorized persons who must register upon entry to the property and must, when requested, display government or other identifying credentials to federal police officers or other authorized individuals when entering, leaving or while on the property. Failure to comply with any of the applicable provisions is a violation of these regulations.

#### **Sec. 102-74.380 Preservation of Property**

All persons entering in or on federal property are prohibited from improperly disposing of rubbish on property, willfully destroying or damaging property, stealing property, creating any hazard on property to persons or things, and throwing articles of any kind from or at a building or the climbing upon statues, fountains or any part of the building.

#### **Sec. 102-74.385 Conformity with Signs and Directions**

Persons in and on property must at all times comply with official signs of a prohibitory, regulatory or directory nature and with the lawful direction of federal police officers and other authorized individuals.

### **Sec. 102-74.390 Disturbances**

All persons entering in or on federal property are prohibited from loitering, exhibiting disorderly conduct or exhibiting other conduct on property which creates loud or unusual noise or a nuisance, unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways or parking lots, otherwise impedes or disrupts the performance of official duties by government employees, or prevents the general public from obtaining the administrative services provided on the property in a timely manner.

### **Sec. 102-74.395 Gambling**

Except for the vending or exchange of chances by licensed blind operators of vending facilities for any lottery set forth in a state law and authorized by section 2(a)(5) of the Randolph-Sheppard Act (20U.S.C.107), all persons entering in or on federal property are prohibited from participating in games for money or other personal property, operating gambling devices, conducting a lottery or pool or selling or purchasing of numbers tickets.

### **Sec. 102-74.400 Narcotics and Other Drugs**

Except in cases where the drug is being used as prescribed for a patient by a licensed physician, all persons entering in or on federal property are prohibited from being under the influence, using or possessing any narcotic drugs, hallucinogens, marijuana, barbiturates or amphetamines; or operating a motor vehicle on the property while under the influence of alcoholic beverages, narcotic drugs, hallucinogens, marijuana, barbiturates or amphetamines.

### **Sec. 102-74.405 Alcoholic Beverages**

Except where the head of the responsible agency or his or her designee has granted an exemption in writing for the appropriate official use of alcoholic beverages, all persons entering in or on federal property are prohibited from being under the influence or using alcoholic beverages. The head of the responsible agency or his or her designee must provide a copy of all exemptions granted to the buildings manager and the highest ranking representative of the law enforcement organization, or other authorized officials, responsible for the security of the property.

### **Sec. 102-74.410 Soliciting, Vending and Debt Collection**

All persons entering in or on federal property are prohibited from soliciting commercial or political donations, vending merchandise of all kinds, displaying or distributing commercial advertising or collecting private debts, except for:

- (a) National or local drives for funds for welfare, health or other purposes as authorized by 5 CFR part 950, entitled "Solicitation of Federal Civilian and Uniformed Service Personnel For Contributions To Private Voluntary Organizations," and sponsored or approved by the occupant agencies.
- (b) Concessions or personal notices posted by employees on authorized bulletin boards.
- (c) Solicitation of labor organization membership or dues authorized by occupant agencies under the Civil Service Reform Act of 1978; and
- (d) Lessee, or its agents and employees, with respect to space leased for commercial, cultural, educational or recreational use under the Public Buildings Cooperative Use Act of 1976 (40 U.S.C. 490(a)(16)). Public areas of GSA-controlled property may be used for other activities in accordance with subpart D of this part.

### **Sec. 102-74.415 Posting and Distributing Materials**

All persons entering in or on federal property are prohibited from:

- (a) Distributing free samples of tobacco products in or around federal buildings, under Public Law 104-52, Section 636.
- (b) Posting or affixing materials, such as pamphlets, handbills or flyers, on bulletin boards or elsewhere on GSA-controlled property, except as authorized in S102-74.410, or when these displays are conducted as part of authorized government activities.
- (c) Distributing materials, such as pamphlets, handbills or flyers, unless conducted as part of authorized government activities. This prohibition does not apply to public areas of the property as defined in S102-71.20 of this chapter. However, any person or organization proposing to distribute materials in a public area under this section must first obtain a permit from the



building's manager as specified in subpart D of this part. Any such person or organization must distribute materials only in accordance with the provisions of subpart D of this part. Failure to comply with those provisions is a violation of these regulations.

### **Sec. 102-74.420 Photographs for News, Advertising or Commercial Purposes**

Except where security regulations apply or a federal court order or rule prohibits it, persons entering in or on federal property may take photographs of:

- (a) Space occupied by a tenant agency for non-commercial purposes only with the permission of the occupying agency concerned;
- (b) Space occupied by a tenant agency for commercial purposes only with written permission of an authorized official of the occupying agency concerned; and
- (c) Building entrances, lobbies, foyers, corridors or auditoriums for news purposes.

### **Sec. 102-74.425 Dogs and Other Animals**

Except seeing eye dogs, other guide dogs and animals used to guide or assist handicapped persons, persons may not bring dogs or other animals on federal property for other than official purposes.

### **Sec. 102-74.430 Vehicular and Pedestrian Traffic**

All vehicle drivers entering or while on federal property:

- (a) Must drive in a careful and safe manner at all times;
- (b) Must comply with the signals and directions of federal police officers or other authorized individuals;
- (c) Must comply with all posted traffic signs;
- (d) Must comply with any additional posted traffic directives approved by the GSA regional administrator, which will have the same force and effect as these regulations;
- (e) Are prohibited from blocking entrances, driveways, walks, loading platforms or fire hydrants; and
- (f) Are prohibited from parking on federal property without a permit. Parking without author-

ity, parking in unauthorized locations or in locations reserved for other persons, or parking contrary to the direction of posted signs is prohibited. Vehicles parked in violation, where warning signs are posted, are subject to removal at the owner's risk and expense. Federal agencies may take as proof that a motor vehicle was parked in violation of these regulations or directives as prima facie evidence that the registered owner was responsible for the violation.

### **Sec. 102-74.435 Explosives**

No person entering or while on federal property may carry or possess explosives, or items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes.

### **Sec. 102-74.440 Weapons**

Federal law prohibits the possession of firearms or other dangerous weapons in federal facilities and federal court facilities by all persons not specifically authorized by Title 18, United States Code, Section 930. Violators will be subject to fine and/or imprisonment for periods up to five (5) years.

### **Sec. 102-74.445 Nondiscrimination**

Federal agencies must not discriminate by segregation or otherwise against any person or persons because of race, creed, sex, color or national origin in furnishing or by refusing to furnish to such person or persons the use of any facility of a public nature, including all services, privileges, accommodations and activities provided on the property.

### **Sec. 102-74.450 Penalties**

A person found guilty of violating any rule or regulation in this subpart while on any property under the charge and control of the GSA shall be fined under Title 18 of the United States Code, imprisoned for not more than 30 days or both.

### **Sec. 102-74.455 Impact on Other Laws or Regulations**

No rule or regulation in this subpart may be construed to nullify any other federal laws or regulations or any state and local laws and regulations applicable to any area in which the property is situated (section 205(c), 63 Stat. 390; 40 U.S.C. 488 (c)).

## U.S. Code, Title 18—Crimes And Criminal Procedure;

### Part I—Crimes;

#### Chapter 44—Firearms

##### Sec. 930. Possession of Firearms and Dangerous Weapons in Federal Facilities

- (a) Except as provided in subsection (d), whoever knowingly possesses or causes to be present a firearm or other dangerous weapon in a federal facility (other than a federal court facility), or attempts to do so, shall be fined under this title or imprisoned not more than one year, or both.
- (b) Whoever, with intent that a firearm or other dangerous weapon be used in the commission of a crime, knowingly possesses or causes to be present such firearm or dangerous weapon in a federal facility, or attempts to do so, shall be fined under this title or imprisoned not more than five years, or both.
- (c) A person who kills any person in the course of a violation of subsection (a) or (b), or in the course of an attack on a federal facility involving the use of a firearm or other dangerous weapon, or attempts or conspires to do such an act, shall be punished as provided in sections 1111, 1112, 1113 and 1117.
- (d) Subsection (a) shall not apply to:
- (1) the lawful performance of official duties by an officer, agent or employee of the United States, a state or a political subdivision thereof, who is authorized by law to engage in or supervise the prevention, detection, investigation or prosecution of any violation of law;
  - (2) the possession of a firearm or other dangerous weapon by a federal official or a member of the Armed Forces if such possession is authorized by law; or
  - (3) the lawful carrying of firearms or other dangerous weapons in a federal facility incident to hunting or other lawful purposes.
- (e)
- (1) Except as provided in paragraph (2), whoever knowingly possesses or causes to be present a firearm in a federal court facility, or attempts to do so, shall be fined under this title, imprisoned not more than two years, or both.
  - (2) Paragraph (1) shall not apply to conduct which is described in paragraph (1) or (2) of subsection (d).
  - (f) Nothing in this section limits the power of a court of the United States to punish for contempt or to promulgate rules or orders regulating, restricting or prohibiting the possession of weapons within any building housing such court or any of its proceedings, or upon any grounds appurtenant to such building.
  - (g) As used in this section:
    - (1) The term “federal facility” means a building or part thereof owned or leased by the federal government, where federal employees are regularly present for the purpose of performing their official duties.
    - (2) The term “dangerous weapon” means a weapon, device, instrument, material or substance, animate or inanimate, that is used for, or is readily capable of, causing death or serious bodily injury, except that such term does not include a pocket knife with a blade of less than 2½ inches in length.
    - (3) The term “federal court facility” means the courtroom, judges, chambers, witness rooms, jury deliberation rooms, attorney conference rooms, prisoner holding cells, offices of the court clerks, the United States attorney and the United States marshal, probation and parole offices and adjoining corridors of any court of the United States.
  - (h) Notice of the provisions of subsections (a) and (b) shall be posted conspicuously at each public entrance to each federal facility, and notice of subsection (e) shall be posted conspicuously at each public entrance to each federal court facility, and no person shall be convicted of an offense under subsection (a) or (e) with respect to a federal facility if such notice is not so posted at such facility, unless such person had actual notice of subsection (a) or (e), as the case may be.

# Appendix 2

## Sample Forms and Reports



### Bomb Threat Questionnaire

#### Questions derived from FBI Bomb Data Program Card

1. When is the bomb going to explode? \_\_\_\_\_
2. Where is it right now? \_\_\_\_\_
3. What does it look like? \_\_\_\_\_
4. What kind of bomb is it? \_\_\_\_\_
5. What will cause it to explode? \_\_\_\_\_
6. Did you place the bomb? \_\_\_\_\_
7. Why? \_\_\_\_\_
8. What is your address? \_\_\_\_\_
9. What is your name? \_\_\_\_\_

**Exact wording of the threat:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Sex of Caller: \_\_\_\_\_ Race: \_\_\_\_\_ Age: \_\_\_\_\_

Length of call: \_\_\_\_\_ Number at which call is received: \_\_\_\_\_

Time: \_\_\_\_\_ Date: \_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_

## Bomb Threat Questionnaire Con't

Caller's Voice:

- |                                  |                                   |                                  |  |
|----------------------------------|-----------------------------------|----------------------------------|--|
| <input type="checkbox"/> Calm    | <input type="checkbox"/> Loud     | <input type="checkbox"/> Nasal   | <input type="checkbox"/> Clearing throat |
| <input type="checkbox"/> Angry   | <input type="checkbox"/> Laughter | <input type="checkbox"/> Stutter | <input type="checkbox"/> Deep breathing  |
| <input type="checkbox"/> Excited | <input type="checkbox"/> Crying   | <input type="checkbox"/> Lisp    | <input type="checkbox"/> Cracking voice  |
| <input type="checkbox"/> Slow    | <input type="checkbox"/> Normal   | <input type="checkbox"/> Raspy   | <input type="checkbox"/> Disguised       |
| <input type="checkbox"/> Rapid   | <input type="checkbox"/> Distinct | <input type="checkbox"/> Deep    | <input type="checkbox"/> Accent          |
| <input type="checkbox"/> Soft    | <input type="checkbox"/> Slurred  | <input type="checkbox"/> Ragged  | <input type="checkbox"/> Familiar        |

If voice is familiar, who did it sound like? \_\_\_\_\_  
\_\_\_\_\_

Background Sounds:

- |  |   |  |  |
|--|---|--|--|
| <input type="checkbox"/> Street noises | <input type="checkbox"/> Music            | <input type="checkbox"/> Factory machinery | <input type="checkbox"/> Local         |
| <input type="checkbox"/> Crockery      | <input type="checkbox"/> House noises     | <input type="checkbox"/> Animal noises     | <input type="checkbox"/> Long distance |
| <input type="checkbox"/> Voices        | <input type="checkbox"/> Motor            | <input type="checkbox"/> Clear             | <input type="checkbox"/> Booth         |
| <input type="checkbox"/> PA System     | <input type="checkbox"/> Office machinery | <input type="checkbox"/> Static            | <input type="checkbox"/> Other         |

Threat Language:

- |   |                                     |   |
|---|-------------------------------------|---|
| <input type="checkbox"/> Well spoken (educated) | <input type="checkbox"/> Irrational | <input type="checkbox"/> Taped                        |
| <input type="checkbox"/> Foul                   | <input type="checkbox"/> Incoherent | <input type="checkbox"/> Message read by threat maker |

Remarks: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date \_\_\_\_/\_\_\_\_/\_\_\_\_

Name \_\_\_\_\_

Position \_\_\_\_\_

Phone number \_\_\_\_\_

## Offense/Incident Report

NOTE: The sample form of the Offense/Incident Report (Form 3155) along with the instructions for completing the form is provided.

Page 80  
Left Blank Intentionally

# Appendix 3

## Practice Written Examination and Answer Key



### Information, Guidelines and Helpful Hints for Taking the Written Examination

FPS wants you to succeed on the written examination. Some information regarding the test is provided for you. We hope it will assist you in preparing for, taking and passing the examination.

#### Before the Examination

- Read and study the Security Guard Information Manual (SGIM), which your employer should provide to you well in advance of you taking the exam. Every question on the test will be taken directly from the SGIM. If you don't read and study the manual, your chances to pass will be much lower.
- Take this practice test. It's identical in format to the actual examination, and the questions are similar in nature to the actual test questions (as with the actual exam, all the practice questions are taken directly from the SGIM).
- The night before the test, try to get plenty of rest. Give yourself adequate time to travel to the testing site. Try to have a healthy meal or snack a couple of hours before the test so that you will be alert and ready to focus on the exam. Make sure you visit the rest room before the test, as you will not be able to leave the examination room once the test begins.

#### The Examination

- Every test contains 50 multiple choice questions. Each question is worth two points, for a total possible score of 100 points. There are no bonus or extra credit questions.
- The passing score is 70 percent, or 35 correct answers out of 50 questions. You can miss 15 questions and still pass the test.

- If you fail the initial exam, you may take the exam one (1) additional time within 90 days from the date of your first attempt.
- You will be given one (1) hour to complete the examination. Since the questions are short, one hour should be more than enough time for you to finish the exam and check your answers before you turn in your test and answer sheet.
- If you do not answer a question, the scanning machine that scores the examination will treat it as an incorrect answer. Therefore, it is to your advantage to make your best guess on every single question. Don't leave any answers blank on the examination.
- With every multiple choice question, there will always be four (4) possible answers.
- On multiple choice questions, look for the answer that best fits the question. One good way to approach multiple choice questions is to use the process of elimination. Many questions will have one possible answer that is clearly wrong. If you are unsure about the best answer, first eliminate the clearly incorrect answers and then try to choose the best remaining answer.
- Some multiple choice questions will require you to choose more than one answer or none of the answers (i.e., all of the above or none of the above). Again, the process of elimination is helpful in answering these questions.
- If you get stuck on a question, make a light pencil mark in the margin next to the question on the answer sheet and move on to the next question. Come back to the question once you've finished the test or when you think of the answer. The chances are high that there will be several questions on a specific topic. Sometimes the answer to

one question may trigger you to remember the answer for another. Make sure you erase the margin mark next to the question once you have answered it so that the scanning machine does not malfunction and try to read the margin mark as an actual answer.

- Relax and take one question at a time. Once you get a feel for the test, you'll find it will be much easier to concentrate and answer the questions.
- You'll find many of the questions are as much about common sense as they are about specific knowledge of the SGIM. If a question seems too technical to you, try to think of it from a common-sense standpoint. Usually your first inclination will be the correct answer. Do not talk yourself into an incorrect answer.
- One of the best things you can do for yourself during the test, especially right before you start or if you feel yourself getting tense, is take a few slow, deep breaths. Tension can make you physically uncomfortable and mentally blocked.
- Be confident! If you have read and studied the SGIM, the chances are very good that you will pass the test on your first attempt.

## Practice Examination

Name: \_\_\_\_\_

To assist you with taking the actual examination, 25 practice exam questions are provided.

1. Which of the below listed is a type of jurisdiction:
  - A. Permanent
  - B. Temporary
  - C. Exclusive
  - D. None of the above
2. The letter "C" in the acronym CYMBL stands for:
  - A. Cost
  - B. Criteria
  - C. Code
  - D. None of the above
3. Which security system would augment a security guard:
  - A. Duress Alarm
  - B. Motion Detector
  - C. Audio Sensor
  - D. All of the above
4. What does a "Code Adam" alert mean:
  - A. Incoming VIPs
  - B. Inoperative government vehicle
  - C. A missing child
  - D. Radio procedures
5. If someone requests a copy of a report you should:
  - A. Disregard the request
  - B. Give them a copy
  - C. Contact the FPS MegaCenter
  - D. None of the above
6. When faced with someone being rude, you should:
  - A. Laugh at them
  - B. Remain professional and courteous
  - C. Threaten them
  - D. Return the gesture
7. A positive reading on a drug test means:
  - A. The guard can go to rehab and still work on the contract
  - B. The test will be disregarded
  - C. Grounds for immediate dismissal and removal
  - D. A waiver can be submitted
8. On matters of physical security, FPS consults with building owners and:
  - A. The public
  - B. Visitors
  - C. The tenants
  - D. No one else
9. An area where a crime occurs is called:
  - A. A hangout
  - B. A setting
  - C. A crime scene
  - D. A backdrop
10. When reporting for duty your uniform should be:
  - A. Folded
  - B. Dirty and soiled
  - C. Not pressed
  - D. Clean and unwrinkled



11. The Pentagon and the CIA are examples of what level facility:
- III—three
  - II—two
  - V—five
  - I—one
12. FPS's policy on sexual harassment is:
- Let the guards work it out
  - Schedule the same sexes to work together
  - They are not concerned
  - It will not be tolerated
13. What are the three classes of fire:
- B, C, & D
  - A, A, & B
  - A, C, & D
  - A, B, & C
14. Which is a category of sabotage:
- Passive
  - Explosive
  - Lethal
  - None of the above
15. Which is an approved form of identification for access purposes:
- None required
  - Drivers license
  - Charge card with no photo
  - All of the above
16. International terrorism involves groups/individuals whose activities are:
- Peaceful
  - Irrational
  - Unfounded
  - Foreign based
17. Before being allowed to carry a firearm you must:
- Explain the weapons nomenclature
  - Complete and pass a range qualification course
  - Buy your own weapon
  - There are no requirements
18. Fires may be set by people for:
- Economic gain
  - Taking revenge
  - To conceal a crime
  - All of the above
19. If you encounter a container with a gaseous substance inside you should:
- Not touch it
  - Report it immediately
  - Not open it
  - All of the above
20. Any threat received over the telephone should be taken:
- Jokingly
  - Disregarded
  - Seriously
  - Lightly
21. On a daily basis, FPS MegaCenters are operational:
- 24 hours
  - 12 hours
  - 8 hours
  - Only at night
22. What is a basic rule of firearm safety:
- Always treat every weapon as if it is loaded
  - Practice quick-draw procedures
  - Keep your holster unsnapped
  - None of the above
23. What is required in order to have a beard while on duty:
- Note from home
  - Medical certificate
  - No paperwork is required
  - Note from your supervisor
24. What is called a violent crime:
- Panhandling
  - Assault
  - Stealing
  - Jaywalking
25. The proper footwear while in uniform is:
- In good condition
  - With closed toes and heels
  - Black with black laces
  - All of the above

## Answer Key

Listed below are the answers to the practice test questions.

Question Number/Answer	SGIM Page
1. C	35
2. D	48
3. D	58
4. C	73
5. C	71
6. B	13
7. C	17
8. C	2
9. C	39
10. D	13
11. C	6
12. D	23
13. D	63
14. B	93
15. B	53
16. D	78
17. B	45
18. D	32
19. D	89
20. C	21
21. A	3
22. A	46
23. B	14
24. B	33
25. D	15

# Appendix 4

## FLETC Use of Force Model (Form SH-8704, Rev. 04/99)

### Introduction

The proper use of force is one of the more critical concerns in contemporary law enforcement. You may be confronted in your law enforcement career with situations that will require you to make split second decisions, some of which may have severe, life threatening consequences for you, the offender and the citizens we serve. Your training at the Federal Law Enforcement Training Center (FLETC) will provide you with the knowledge and skills to assist you in making critical decisions about proper force utilization and control.

One of the major objectives of the training at the FLETC is to provide current and relevant instructional material related to the proper utilization of force. Towards this goal, we include a review of the Use of Force model. The model is designed to assist you in developing the necessary skills when directed toward situational circumstances, the action(s) of the subject(s) and the reasonableness of your selected response.

The primary goal of the officer's effort is to gain and maintain control of the subject. Ideally, each enforcement encounter results in a "balanced" utilization of force flowing in the form of escalation, stabilization or de-escalation. The utilization of force is based upon the threats presented and the subject's degree of compliance or noncompliance.

The application of force during an officer/subject encounter should be based primarily on the perceived action(s) of the suspect and not on the actor(s) with whom you are dealing.

Status, notoriety, reputation and friendship should not be a part of the decision making process. An officer's response to a subject's perceived actions



must be guided by objective reasonableness when effecting lawful control.

### Use of Force Model

For the past decade, the FLETC has adopted an integrated approach in the education and training of law enforcement officers in the use of force issues. The model incorporates the three elements the U.S. Supreme Court identified as critical in the determination of the "objective reasonableness" of force utilization. This standard asks whether the officer's actions are objectively reasonable in light of the facts and circumstances confronting the officer and not whether the officer's subjective intent or motive was evil or good. Any inquiry into the reasonableness of an officer's actions will view his use of force in light of the facts and circumstances confronting him, without regard to his underlying intent or motivation.

These elements are incorporated into three facets of the model: the officer's reasonable perception of the situation and risks (Officer Perception) and the officer's perception of the subject's actions (Subject Action) should determine the officer's selected force response (Office Response).

### Officer Perception

The perception of a threat by an officer has often been associated with the color spectrum. The five officer perception levels and their color counterparts include:

1. **Strategic**—the professional officer is engaged in duties with an occupationally produced perception of responsibilities and risks. The broad foundation of the model is represented

by the blue baseline of the color-keyed assessment spectrum.

2. **Tactical**—Here the officer perceives an increase in risks within the confrontational environment, evolving into a procedural process and the development of tactics. The second level of the model is depicted by the color green.
3. **Volatile**—The officer perceives the situation escalating and the level of noncompliance has increased. The color yellow on the model indicates an activated level of alertness in which specific risks are identified by the officer.
4. **Harmful**—The perception of danger has accelerated for the officer and there is a more directed focus on officer safety and defense. The color orange represents the level of the model.
5. **Lethal**—The potentially lethal degree of risk is the most infrequent, and yet most critical for officer safety and survival. The highest level on the model correlates to the most intense color in the threat assessment spectrum, red.

## Subject Action

The left side of the model identifies the five subject action levels judged from the “perspective of the reasonable officer,” “with circumstances that are tense, uncertain and rapidly evolving,” Graham vs. Connor, 490 US 386 (1989).

These five levels include:

1. **Compliant (Cooperative)**—This level represents the vast majority of officer/subject encounters. The likelihood of a physical response by the subject is minimal. The officer can control the situation by using officer presence and verbalization skills.
2. **Resistant (Passive)**—The remaining four levels of subject action are various levels of noncompliance. The subject exhibits the preliminary level of noncompliance that requires some degree of physical contact by the officer in order to elicit compliance. For example, a subject verbally refuses to go with the officer fol-

lowing a lawful arrest. The subject offers no physical or mechanical enhancement toward the resistance effort other than to stand motionless or remain seated.

3. **Resistant (Active)**—At this level, the scope and intensity of the subject’s resistance has increased. The subject is exhibiting physical or mechanical defiance to the officer’s control. For example, during an arrest, the subject turns and walks away from the officer. The subject is using physical energy directed away from the officer. Another example would be if several subjects interlocked their arms together in an act of civil disobedience. The subjects would be perceived at the resistant (active) level on the model because the subjects are using force and/or energy to maintain resistance.
4. **Assaultive (Physical Injury)**—The officer has the perception of an attack or the potential for such an attack on the officer or others. The officer makes the reasonable assessment that such actions by the subject would not result in death or serious physical injury to the officer or others. An example would be during a lawful arrest, the subject walks away from the officer after being given verbal commands to stop. The subject suddenly turns and runs towards the officer with clenched fists to strike the officer and cause physical injury.
5. **Assaultive (Serious Physical Injury/Death)**—The highest level of noncompliance is the least encountered but poses the most serious threat to officer safety. The officer’s objective, reasonable assessment is such that assaultive actions pose an imminent danger by the subject that could result in death or serious physical injury to the officer or others. A subject is holding hostages in a barricade situation. The subject is threatening to kill innocent victims if his demands are not met. If the subject is not stopped, innocent citizens and police officers could be seriously injured or killed.

## Officer Response

The right side of the model identifies the five officer response levels. It should be noted that any response from a lower level can be utilized at any of the above levels if selected by the officer. These levels include the following:

- **Cooperative Controls**—This level includes methods to preserve officer safety and survival, including: officer presence, communications skills, restraint applications, etc. It is important to recognize that the cooperative controls can also be used at all levels within the model in addition to those tools identified throughout the model. For instance, communication skills can be used in an assaultive confrontation by telling the suspects to “Stop,” “Get down,” etc.
- **Contact Controls**—When confronted with a subject demonstrating resistant behavior, the officer uses low-level physical tactics to gain control and cooperation. These tactics can be psychologically manipulative as well as physical, and can include additional verbal persuasion skills, relative positioning strategies and escort positions. For example, if a person who is to be placed under arrest refuses to cooperate with the officer, but remains at the lowest end on the resistance scale and is passive in refusal, the officer would most likely respond with soft empty hand control. The officer may await backup officers and show strength in numbers.
- **Compliance Techniques**—When the subject becomes actively resistant, the officer uses physical control tactics. These tactics should be of sufficient force to overcome the active resistance of the subject and the officer should remain vigilant for more aggressive behavior from the subject. Examples include come-along holds, pressure point applications, joint locks, takedowns and chemical agents.
- **Defensive Tactics**—At this level, the subject attempts or achieves an assault on the officer or another person. The officer is justified in using defensive countermeasures designed to cease the subject’s non-lethal assault on the officer or oth-

ers, regain control and assure continued compliance. These tactics include baton strikes, striking and blocking techniques, etc.

- **Deadly Force**—When the officer perceives that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person, immediate countermeasures must be used to stop the threat. These tactics could include the discharge of a firearm and other forms of deadly force.

## Color Correlation

As is evident, color is a significant component of the Use of Force Model. The colors (blue, green, yellow, orange and red) were drawn from the scientifically supported sequencing of the basic light spectrum, and provide for specific color correlation throughout the model.

- **Control Superiority Principle**—As one looks at each level of the model, it is evident that the color of the officer response side of the model is brighter or more intense. This increase in color intensity is used to facilitate the principle that the officer is always superior to the subject’s degree of compliance/noncompliance in terms of controlled and balanced force utilization.
- **Officer Assessment/Selection Arrows**—The double-headed arrows are used to indicate the dynamic nature of an officer’s decision-making process during an enforcement encounter. The subject may escalate, stabilize or de-escalate his degree of noncompliance during the confrontation; so too, the officer must be able to practice flexibility in force responses to match the threat.
- **Survival Shadow**—The officer assessment and selection arrows are bordered with a red line to indicate that the officer’s occupation is of high risk. The officer must be constantly reminded that imminent danger causing death and/or serious physical injury can occur at any time.

## Tools, Tactics and Timing

**Tools** are the mechanical, physical or mental resources we have in order to promote or gain compliance. These include the curriculum topics such as intermediate/lethal weapons, weaponless control techniques and survival mind-set. The officer may rely on a variety of tools in response to an enforcement situation.

**Tactics** are the applications of these tools in the form of techniques, procedures, etc. The officer must incorporate the tools into strategies to accomplish an arrest, such as keeping the subjects hands visible at all times or the proper use of cover or concealment.

**Timing** is the correlation of tools and tactics to produce the timely and effective application of the appropriate level of force required to establish and maintain lawful control. An example is when an officer applies handcuffs during an arrest in order to minimize the potential of an assault on the officer.

Inside Back Cover  
Left Blank Intentionally



# U.S. Immigration and Customs Enforcement

Report Suspicious Activity  
to the FPS MegaCenter:  
**1-877-4FPS-411**  
(1-877-437-7411)  
[www.ice.gov](http://www.ice.gov)