Workplace Security

Introduction

Law enforcement and security officers should be involved in all stages of the planning process in an effective workplace violence prevention program. They can play an active role in prevention, intervention, and response to threatening situations, in addition to their traditional role of responding to actual incidents of physical violence. This section will provide general ideas and considerations that can help the agency planning group gain an understanding of some of the law enforcement/security issues such as jurisdiction. It is also intended to help those Federal offices that do not have in-house security or law enforcement identify the appropriate organizations that can assist them.

Security Planning

Depending on the agency, location of the office, and the type of incident or situation, jurisdiction may vary. The agency's own law enforcement organization, the Federal Protective Service (FPS), or Federal, state, or local law enforcement, or a combination of these, may have jurisdiction. There also may be gaps in law enforcement coverage when issues of workplace violence arise. These gaps can be closed if the agency planning group (which would include any in-house security organization) works with the various law enforcement organizations in setting up workplace violence programs. The following are some suggestions for involving law enforcement in agency efforts to prevent workplace violence.

Jurisdiction

The agency planning group should identify which Federal or local law enforcement agency or agencies have responsibility for its worksite. For example, the FPS is the primary law enforcement service for responding to incidents in Federal facilities under the charge and control of the General Services Administration (GSA) as an owned or leased facility. FPS typically locates its offices in areas where there is a high concentration of Federal employees and is capable of providing timely responses to GSA owned or leased facilities in these areas. For immediate responses to GSA owned or leased facilities in rural areas and/or areas with a small Federal presence, law enforcement officials from local jurisdictions should be contacted.

Security Planning (continued)

Some agencies have in-house security and/or law enforcement organizations. Others have contracts with private security firms. It is not always clear who has jurisdiction, and who should be contacted when the need arises.

Sometimes meeting with the local police chief, county sheriff, or state police is necessary to establish a plan or procedure regarding law enforcement response in the event of potential violence or hostile incidents. Sometimes new building agreements will be necessary or contracts will have to be modified. In remote locations, arrangements can be made for local police to handle certain situations until the appropriate Federal law enforcement officials arrive.

Liaison with law enforcement agencies

The agency planning group, and later the incident response team, should maintain open and continuous liaison with those law enforcement agencies responsible for their worksite. This would entail having periodic meetings to discuss the agency's concerns. Without these contacts, lines of communication can break down and misunderstandings could arise. It is during these contacts that the agency can obtain the names and telephone numbers of law enforcement personnel to be called upon should the need arise. Planning groups in agencies that already have established liaisons should work through these established liaisons to avoid confusion.

Know in advance which Federal or local law enforcement agency or agencies have jurisdiction over your worksite. Involve them early in the planning process.

Law Enforcement and Security Assistance

During the planning phase, law enforcement/security officers can:

- Identify types of situations they can address and when and how they should be notified of an incident;
- Indicate whether their officers have arrest authority;
- Identify their jurisdictional restrictions and alternative law enforcement agencies that may be able to provide assistance;

Law Enforcement and Security Assistance (continued)

- Identify threat assessment professionals who can assist the agency in its efforts to protect threatened employees;
- Advise on what evidence is necessary and how it can be collected or recorded, so that law enforcement can assess the information and decide what action to take, if appropriate;
- Explain anti-stalking laws applicable in the agency's jurisdiction and how and when to obtain restraining orders;
- Suggest security measures to be taken for specific situations, such as in cases where Employee Assistance Program counselors or other mental health professionals warn the agency that an individual has made a threat against an agency employee; and
- Arrange for supervisor/employee briefings or training on specific workplace violence issues such as:
  - Personal safety and security measures;
  - Types of incidents to report to law enforcement/security;
  - Types of measures law enforcement/security may take to protect employees during a violent incident, e.g., explanations of what it means to "secure the area," "secure the perimeter," and "preserve evidence";
  - Suggestions on how to react to an armed attacker;
  - Suggestions for dealing with angry customers or clients;
  - Suspicious packages;
  - Bomb threats;
  - Hostage situations; and
  - Telephone harassment and threats.

When potentially violent situations arise, law enforcement/ security officers can work with the incident response team to:

- Provide an assessment of the information available to determine whether law enforcement intervention is immediately necessary; for example, whether a criminal investigation is appropriate and whether a threat assessment professional should be consulted;
- Identify what plan of action they deem appropriate; and
- Determine who will gather what types of evidence.

Physical Security Measures

Many Federal agencies have numerous security measures in place that can reduce the risk of workplace violence. These include closed circuit cameras, silent alarms, metal detectors, two-way mirrors, electronic access systems, barriers to prevent cars from driving too close to the building, emergency internal code words, extra lighting in the parking lots, and escorts to and from parking lots after dark. Planning groups should review security measures and procedures and make recommendations for modifications and improvements as necessary.

The U.S. Department of Justice, U.S. Marshals Service, has issued a publication containing recommendations for increasing security in Federal facilities. Entitled *Vulnerability Assessment of Federal Facilities*, it can be obtained by contacting the U.S. Government Printing Office, Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328 (Publication # 027-000-01362-7).

The information in the following section regarding physical security has been provided by the General Services Administration's (GSA) Federal Protective Service.

> If your agency is not in GSA owned or leased buildings, you can obtain the same type of assistance from the law enforcement or security organization that has jurisdiction over your worksite.

Physical Security in GSA Owned or Leased Buildings

There are more than 900,000 employees working in approximately 6,800 GSA owned or leased Federal buildings. GSA is the agency responsible for ensuring the safety and security of people while on Federal property that is owned or leased by GSA. This section contains recommendations and requirements for agencies in GSA controlled or leased space.

Regulations

Federal Property Management Regulations 41 CFR Part 101-20 and Executive Order 12656 specifically require GSA to provide standard protection services by coordinating a comprehensive Occupant Emergency Program, which is a short-term emergency response program establishing procedures for safeguarding lives and property during emergencies.

Physical Security in GSA Owned or Leased Buildings (continued)

GSA designated official

Each GSA owned or leased facility has a designated official, who is the highest ranking official of the primary occupant agency of a Federal facility, or alternatively, a designee selected by mutual agreement of occupant agency officials. The designated official is responsible for developing, implementing, and maintaining an Occupant Emergency Plan, which consists of procedures developed to protect life and property in a specific Federally occupied space under stipulated emergency conditions. The designated official's responsibilities include establishing, staffing, and training an Occupant Emergency Organization, comprised of agency employees who have been designated to perform the requirements established by the Occupant Emergency Plan.

According to the regulations, the GSA must assist in the establishment and maintenance of such plans and organizations. All agencies occupying a facility must fully cooperate with the designated official in the implementation of the emergency plans and the staffing of the emergency organization. GSA must provide emergency program policy guidance, review plans and organizations annually, assist in training of personnel, and otherwise ensure proper administration of Occupant Emergency Programs. In leased space, GSA will solicit the assistance of the lessor in the establishment and implementation of plans.

According to the regulations, decisions to activate the Occupant Emergency Organization shall be made by the designated official, or by the designated alternate official. Decisions to activate shall be based upon the best available information, including an understanding of local tensions, the sensitivity of target agencies, and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA buildings manager, from the appropriate Federal Protective Service official, and from Federal, State, and local law enforcement agencies.

Physical Security Survey

A major goal of the GSA's Federal Protective Service is to provide better protection for Federal employees and visitors by pinpointing high-risk areas in Federal buildings where potential problems or emergency situations might occur. This is accomplished through a "Physical Security Survey" conducted by a certified GSA physical security specialist. The survey is a comprehensive, detailed, technical on-site inspection and analysis of the current security and physical protection conditions.

If your agency does not have up-to-date security procedures in place, the head of your agency may want to ask a regional GSA Federal Protective Service office or your agency's security office to conduct a physical security survey to ensure that employees are working in a safe and secure environment. There is a listing of Federal Protective Service offices at the end of this section on page 131.

The following are some examples provided by the FPS of ways to improve security in your office and/or building.

- Post a security guard at the main building entrance or at entrances to specific offices.
- Install a metal detector or CCTV (closed-circuit television) camera or other device to monitor people coming in all building entrances.
- Issue all employees photo identification cards and assign temporary passes to visitors, who should be required to sign in and out of the building. Under certain conditions, contract guards should be required to call Federal offices to confirm an appointment and/or to request an escort for all visitors — customers, relatives, or friends.
- Brief employees on steps to take if a threatening or violent incident occurs. Establish code words to alert coworkers and supervisors that immediate help is needed.
- Install silent, concealed alarms at reception desks.

The following are some examples provided by the FPS of ways to improve security in "front-line" offices that serve the public.

Physical Security Survey (continued)

- Ensure that officers (or guards) should have a clear view of the customer service area at all times.
- Arrange office furniture and partitions so that front-line employees in daily contact with the public are surrounded by "natural" barriers (desks, countertops, partitions) to separate employees from customers and visitors.
- Provide an under-the-counter duress alarm system to signal a supervisor or security officer if a customer becomes threatening or violent.
- Establish an area in the office for employees and/or customers to escape to if they are confronted with violent or threatening people.
- Provide an access-control combination lock on access doors.
- Mount closed circuit television cameras for monitoring customer service activity from a central security office for the building.

More examples of measures agencies can take to improve security for its employees can be found in the publications by the Federal Protective Service, National Institute for Occupational Safety and Health, and Occupational Safety and Health Administration that are listed in Part IV.

Computer Security

Agency planning groups should address ways to safeguard computer systems. There have been cases where employees have sabotaged computer equipment, computer systems, and computer records. Therefore, whenever a threat of sabotage is suspected, procedures should be initiated to prevent the person from having access to the facility's computer system.

It is important to act quickly whenever there is reason to believe that an employee or ex-employee may commit such an act. It is standard practice to collect IDs, building passes, keys, and parking passes when employees leave their jobs. Often, however, no one thinks to block access to computer systems or networks.

Computer Security (continued)

Some agencies, when terminating employees, bar them from the premises and eradicate their passwords to computer systems that are accessible from outside the premises.

> *"The agency planning group, as part of the response plan, should talk to the information/computer security officer or computer system administrators to determine the vulnerability of the computer networks and the procedures that need to be implemented to lock individuals out of these systems."*

This type of access information is sometimes difficult to determine; often, it is not readily available in one central place. For example, information technology administrators may know who has access to various computer systems, and the facilities manager may know who has access to the computer systems that control the building's heating, air-conditioning, and other support functions for the facility. The agency planning group, as part of the response plan, should talk to the information/computer security officer or computer system administrators to determine the vulnerability of the computer networks and the procedures that need to be implemented to lock individuals out of these systems.

Examples of Handouts

The following pages contain examples of handouts developed by the Federal Protective Service (FPS) that can be used by or adapted for your agency. FPS regional offices, listed on page 131, may be contacted for additional brochures and literature on office safety and security.

Examples of Useful Handouts for Employees

The attached desk card summarizes the actions you should (or should not) take in a hostile or threatening situation. Print out and detach the card, tear or cut along the dotted lines, fold the card into a "tent," and tape the ends together underneath so that the card will stand up on your desk with the text facing you. Review the card often. That way, if you are confronted by an angry, hostile, or threatening customer or coworker, you will know what you should do. Everyone in your office, including supervisors and managers, should follow these same procedures. You can make copies of this card so that everyone has his or her own card.

Coping With Threats and Violence

For an angry or hostile customer or coworker

- Stay calm. Listen attentively.
- Maintain eye contact.
- Be courteous. Be patient.
- Keep the situation in your control.

For a person shouting, swearing, and threatening

- Signal a coworker, or supervisor, that you need help.
  (Use a duress alarm system or prearranged code words.)
- Do not make any calls yourself.
- Have someone call the FPS, contract guard, or local police.

For someone threatening you with a gun, knife, or other weapon

- Stay calm. Quietly signal for help.
  (Use a duress alarm or code words.)
- Maintain eye contact.
- Stall for time.
- Keep talking — but follow instructions from the person who has the weapon.
- Don't risk harm to yourself or others.
- Never try to grab a weapon.
- Watch for a safe chance to escape to a safe area.

Federal Protective Service
U.S. General Services Administration

Handy Reference Card

Everyone in your office, including supervisors and managers, should follow these same procedures. Make copies of the card if you need to so everyone will have his or her own card.

Telephone Threats

- Keep calm. Keep talking.
- Don't hang up.
- Signal a coworker to get on an extension.
- Ask the caller to repeat the message and write it down.
- Repeat questions, if necessary.
- For a bomb threat, ask where the bomb is and when it is set to go off.
- Listen for background noises and write down a description.
- Write down whether it's a man or a woman; pitch of voice, accent; anything else you hear.
- Try to get the person's name, exact location, telephone number.
- Signal a coworker to immediately call the FPS, a contract guard, or the local police.
- Notify your immediate supervisor.

Federal Protective Service
U.S. General Services Administration

Emergency Phone Numbers

Carefully tear out the "Emergency Phone Numbers" card at the dotted lines. Write in all the emergency numbers for your building. Tape this card on your desk by your phone or somewhere else close to your phone for handy reference. (Copies of this card also can be made.)

Federal Protective Service_____

Building Security_____

Police/Sheriff_____

Fire Department_____

Ambulance_____

Health Unit_____

Federal Protective Service
U.S. General Services Administration

Federal Protective Service Offices

For more information on coping with threats and violence in Federal Offices, other crime prevention, security surveys, and protection assistance, write or call your nearest Federal Protective Service, Public Buildings Service, U.S. General Services Administration at one of these regional addresses.

Washington, DC Metropolitan Area: Southeast Federal Center, 3rd & M Streets S.E., Washington, DC 20407-0001, (202) 690-9632

Connecticut, Maine, Massachusetts, New Hampshire, Vermont, Rhode Island: 10 Causeway Street, Room 108, Boston, MA 02222-1098, (617) 565-5776

New York, New Jersey, Puerto Rico, U.S. Virgin Islands: 26 Federal Plaza, New York, NY 10278-0013, (212) 264-4255

Delaware, Maryland and Virginia (except Washington DC Metropolitan area), Pennsylvania, West Virginia: 100 Penn Square East, Philadelphia, PA 19107-3396, (215) 656-6043

Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee: 401 West Peachtree Street, NW, Atlanta, GA 30365-2550, (404) 331-5132

Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin: 230 South Dearborn Street, Chicago, IL 60604-1503, (312) 353-1496

Iowa, Kansas, Missouri, Nebraska: 1500 Bannister Road, Kansas City, MO 64131-3088, (816) 926-7025

Arkansas, Louisiana, New Mexico, Oklahoma, Texas: 819 Taylor Street, Fort Worth, TX, 76102-6105, (817) 334-3559

Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming: Building 41, Denver Federal Center, Denver, CO 80225-0546, (303) 236-5869

Arizona, California, Hawaii, Nevada, Guam, U.S. Trust Territory of the Pacific: 450 Golden Gate Avenue, San Francisco, CA 94102-3400, (415) 522-3440

Alaska, Idaho, Oregon, Washington: 400 15th Street, SW, Auburn, WA 98001-6599, (206) 931-7529

Crime Prevention Program: 18th & F St. NW, Washington, DC 20405-0002, (202) 501-0907

Case Studies 1, 2, 4, 5, 6, 7, 9, 10, 11, and 13 provide practical examples of some of the issues discussed in this section.