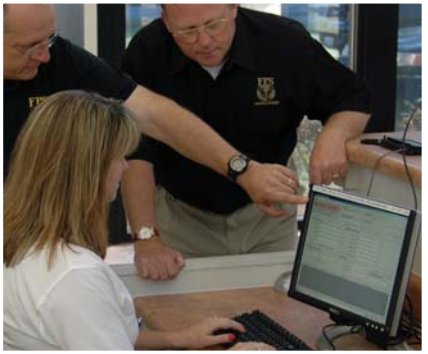

Federal Protective Service

Personal Security Guide

Secure Facilities, Safe Occupants

U.S. Immigration and Customs Enforcement

Message from the Director, Federal Protective Service

Workplace violence, as defined by the Occupational Safety and Health Administration, is violence or the threat of violence against workers. It can occur at or outside the workplace and can range from threats and verbal abuse to physical assaults and homicide, one of the leading causes of job-related deaths.

Those in the legal and public service sectors are at high risk of victimization as a result of their direct contact with members of the public. The members of the public with whom you come into contact are usually there because of some misfortune or other problem, i.e., unemployment, disability, arrest. Each year, the Federal Protective Service (FPS) investigates hundreds of threats directed at federal employees and facilities. When an individual makes implied or specific threats, acts disorderly, communicates inappropriately or engages in other inappropriate behavior that causes you to feel uncomfortable, promptly notifying FPS will assist us in adequately assessing the threat, conduct a timely investigation and employ mitigation strategies to redirect the subject's focus and defuse the situation.

However, the investigative techniques and protective response measures used by FPS in response to a threat are not substitutes for practical steps that an individual can take to minimize their personal risk when away from the workplace. The purpose of this guide is to offer some common sense and proactive measures that *you* and your family can take in an effort to reduce the likelihood of victimization.

Gary W. Schenkel
Director
Federal Protective Service

Table of Contents

Introduction

According to the National Institute for Occupational Safety and Health an average of 1.7 million people were victims of violent crime while working or on duty in the United States each year from 1993 through 1999. This includes 1.3 million simple assaults, 325,000 aggravated assaults, 36,500 rapes and sexual assaults, 70,000 robberies and 900 homicides, a yearly average of over 800 workplace homicides.

This guide has incorporated information from many sources and is offered as an aid for persons who could become victims of targeted violence. An important point to remember is that in order for FPS or other law enforcement agencies to prevent targeted violence and identify, assess and manage potential attackers, there must be a collaborative effort among employees, law enforcement at all levels of government, security organizations, mental health and social services agencies and the private sector.

While this guide discusses what FPS is doing to protect federal employees and visitors, more importantly, it provides safety and personal security recommendations that you can use to improve your security at home or when you travel.

Personal security consists of:

- being aware of locations and situations that would make you vulnerable to criminal victimization, e.g., alleys, dark parking areas, known high-crime areas or traveling alone;
- always being alert and aware of people around you and trust your instincts, e.g., if something in your surroundings doesn't look quite right or someone makes you feel uncomfortable, it probably isn't right; and
- continuing to educate yourself by reviewing this guide and following the advice contained herein.

Protective Investigations Program

FPS established a Protective Investigations Program in early 2004 to enhance the safety of government facilities, employees and visitors. The objective of the program is to prevent an attack on persons and facilities protected by FPS. The program integrates the following aspects of the FPS mission:

- initial patrol response by FPS uniformed police officers;
- full investigation and threat assessment by our special agents;
- prosecution by the U.S. Attorney's Office or State Prosecutor's Office;
- physical security enhancements and countermeasures;
- security briefings and workplace violence seminars administered by FPS law enforcement personnel; and
- suspicious surveillance detection initiatives designed to detect pre-incident indicators of threats to persons and facilities.

FPS special agents conduct investigations and make arrests of subjects charged with making threats to members of the U.S. Congress or their staff, members of the military reserve, Social Security Administration, the Department of Veterans Affairs, the Department of Homeland Security officials and other federal government employees. Many of these investigations result in convictions for making threats to do physical harm and threats to bomb federal facilities.

Additionally, the program is designed to reach out to and educate the community, as well as tenant agencies, and provide them with a point of contact to report suspicious behavior and incidents that threaten persons and federal facilities protected by FPS.

Operation Street Talk

Operation Street Talk is a crime prevention initiative designed to inform, educate and enlist the assistance of persons who may witness suspicious activities affecting federal facilities and employees. This crime prevention initiative, established in 2005, provides information on what to look for and who to call, and is meant to prevent potential terrorist and criminal activity. This program is introduced as part of FPS crime prevention/awareness seminars provided to tenant agencies located in federally owned and leased space. Additionally, FPS law enforcement personnel make contact with local merchants adjacent to federally owned and leased space to engage their assistance in reporting suspicious activity. FPS has published a brochure for this program, which outlines the type of information needed and a toll-free number to call to report the information.

The categories of information contained within the brochure are:

- surveillances;
- elicitations;
- tests of security;
- dry runs;
- suspicious persons;
- deployment of assets; and
- general awareness.

The toll-free number to contact to report suspicious activity is **1-877-4FPS-411** (1-877-437-7411).

The Operation Street Talk brochure is available by calling 202-732-8000.

What You Can Do to Help FPS Protect You

One of the keys to preventing targeted violence is identifying key pieces of information, behavior and actions and notifying FPS in a timely manner so that we may assess the information and determine a course of action designed to defuse the potential for violence. Additionally, you should immediately notify FPS of inappropriate activity, specifically communications received by telephone, facsimile, electronic mail, third party, verbal communication or in writing.

Many criminals target favorite areas and have predictable methods of operation. In many cases, it is information provided by victims and witnesses that leads to the arrest of a criminal or the prevention of a crime. However, at least one out of two crimes in the United States goes unreported, either because people don't think law enforcement can do anything about it or because people don't want to get involved. Everyone should consider it his/her responsibility to report crime and suspicious activity. When you report all the facts about a crime, it helps law enforcement assign resources in the places where crimes are occurring or where they are most likely to occur. If you don't report crime, the criminal can continue to operate without interference.

Examples of Inappropriate Activity or Communications

- Assault or attempted assault on an official.
- Any threats, whether direct, specific, veiled or conditional, e.g., "you'll get yours," "you better do _____ or I will _____."
- An extraordinary complaint or sense of outrage over the handling of an issue.
- References to a special history, destiny or relationship shared with the official.
- Obsessive or stalking behavior, or research on the personal affairs of the official.
- Religious or historical themes involving the official.
- References to death, suicide, weapons, violence, assassinations, acts of terrorism or war.
- Expressions of extreme or obsessive admiration or affection.
- Belief that the official owes the person a debt.
- Perception that the official is someone other than himself/herself, e.g., imposter, God, the Devil, etc..
- Reference to public figures who have been attacked, e.g., Abraham Lincoln, John F. Kennedy, etc..
- References to individuals who have attacked public figures or committed notorious acts of violence or terrorism, e.g., Timothy McVeigh, Lee Harvey Oswald, etc..
- References or claims of mental illness, e.g., psychotic, sociopathic tendencies, etc..
- References to bodyguards, security, safety, danger, etc..
- Bizarre or unreasonable solicitations.
- Suspicious behavior around federal facilities or employees, e.g., vandalism, suspicious inquiries.

Personal Information Security

Today's highly mobile and increasingly electronic world dictates that individuals must be aware of security threats beyond physical security. Personal information is readily available today through private sector companies that compile personal/public information and profit by making the information available to customers/clients for a fee. The following are ways that you can attempt to minimize the availability of personal information in commercial databases.

Do Not Call List

- The Federal Trade Commission (FTC) offers information about the national "do not call" list at: www.ftc.gov/donotcall

Opting Out of Pre-Approved Credit and Other Promotional Offers

- The three major credit bureaus offer a toll-free number (1-888-5-OPTOUT) that enables you to "opt out" of having pre-approved credit offers sent to you for two years

You can notify the three major credit bureaus that you do not want personal information shared for promotional purposes—an important step toward eliminating unsolicited mail. Send your letter to each of the three major credit bureaus as listed below:

- Equifax, Inc. Options, P.O. Box 740123, Atlanta, GA 30374-0123 (www.equifax.com)
- Experian Consumer Opt-Out, 701 Experian Parkway, Allen, TX 75013 (www.experian.com)
- TransUnion Name Removal Option, P.O. Box 505, Woodlyn, PA 19094 (www.transunion.com)

Public Records

Westlaw and Lexis-Nexis both provide online access to public records and publicly available information compiled by third parties from various sources. Neither organization is required by law to comply with opt out requests, however, generally, if you fall into one of the following categories, you may request that your personal identifying information be removed from their directories:

- you are a judge or public official and your position exposes you to a threat of death or serious bodily harm; or
- you are a victim of identity theft.

You will need to provide a written explanation substantiating your request, and in some cases, you will need to provide supporting documentation from law enforcement regarding your situation, i.e., risk of physical harm, identity theft, law enforcement official.

Submit opt out letters to:

- Westlaw Public Records ATTN: D5-S400-Name Removal Request, 610 Opperman Drive, Eagan, MN 55123 E-mail questions to: west.privacypolicy@thomson.com
- Lexis-Nexis Opt-Out, P.O. Box 933, Dayton, Ohio 45401, or via fax at: 1-800-732-7672

Identity Theft

Identity theft can involve the taking of key pieces of personal identifying information, which may include a name, address, date of birth, social security number and/or mother's maiden name, to gain access to a person's financial accounts. Armed with this information, an identity thief may open new credit or financial accounts, buy cars, apply for loans or Social Security benefits, rent an apartment or set up utility and phone service in someone else's name.

The Federal Trade Commission estimates that as many as 9 million people are the victims of some form of identity theft each year. Several steps that you can take to prevent becoming a victim include:

- obtain a copy of your credit report from each of the three credit reporting agencies on a frequent basis, i.e., at least every six months;
- report lost or stolen credit and debit cards, as well as driver's licenses to the appropriate company or department of motor vehicles, as soon as possible;
- closely monitor bank, credit card and investment account statements and look for signs of possible identity theft;
- avoid sharing personal information with persons or businesses that don't have a right to know;
- purchase a cross-cut shredder for your home and use it to shred all mail and correspondence containing personal information; credit card, bank and investment account numbers; name, address, date of birth, SSN, etc.; and
- mail all bill payments at a U.S. Post Office or place in a blue U.S. Postal Service collection box; never place bill payments in your home mailbox to be picked up by whomever decides to steal your outgoing mail.

What to Do if You Think You May Have Become a Victim of Identity Theft

- If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission (SEC) (www.sec.gov/complaint.shtml).
- If you believe someone is using your SSN to apply for a job or to work, report it to the SSA's Fraud Hotline at 1-800-269-0271. Also call SSA at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, and to request a copy of your Social Security statement (www.ssa.gov).
- If an identity thief has established new phone service in your name; is making unauthorized calls that seem to come from, and are billed to, your cellular phone; or is using your calling card and personal identification number (PIN), contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs.
- If you are having trouble getting fraudulent phone charges removed from your account, contact your state Public Utility Commission for local service providers or the Federal Communications Commission (FCC) for long-distance service providers and cellular providers at 1-888-CALL-FCC (www.fcc.gov/ccb/enforce/complaints.html).
- If you suspect that your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your state department of motor vehicles. If your state uses your SSN as your driver's license number, ask to substitute another number.

Computer Security

In today's high technology/global economy, knowledge of cyber-security vulnerabilities and mitigation strategies are part of any security awareness program. Some basics with which to begin include the following:

- use anti-virus software and keep it up to date;
- do not open e-mails or attachments from unknown sources;
- be suspicious of any unexpected e-mail attachments even if they appear to be from someone you know;
- protect your computer from Internet intruders by using a firewall;
- regularly download security updates and patches for operating systems and other software;
- use hard-to-guess passwords with a combination of uppercase and lowercase letters, numbers and special characters and ensure they are at least eight characters long;
- regularly back-up your computer data on disks or CDs;
- Do not share access to your computer with strangers and learn the risks of file sharing;
- disconnect from the Internet when not in use; and
- make sure your family members and/or your employees know what to do if your computer becomes infected.

Additionally, the U.S. CERT Web site (www.us-cert.gov) includes extensive information related to computer security that is broken down into four main categories: Technical Users, Non-Technical Users, Government Users and Control Systems Users. The Non-Technical Users category is geared toward providing security tips to home, corporate and new users and is especially useful for the basic "user of technology." Familiarizing yourself and family members with this information will not only protect your home computer system, but will protect whatever personal information you maintain on your home computer.

At Home

Property crime makes up about three-quarters of all crime in the United States. Overall, in about 83 percent of all burglaries, the offender gained entry into the victim's residence or other building on the property. The following measures may reduce the likelihood of victimization for you and your family:

Trust Your Instincts and Knowledge of Your Surroundings

- Be aware of unexpected changes in and around your home; be suspicious if anything is out of place or does not look right.
- Know who belongs in your neighborhood and who does not; familiarize yourself with vehicles in your neighborhood and their normal location.
- Confirm the identity of utility/service personnel before allowing them admittance to your home.
- Be alert when approached by peddlers or strangers.
- Refuse unordered packages.
- Remain cautious of inquiries regarding the whereabouts or activities of family members. Instruct family members, particularly children, on what kind of information not to divulge.

Good Security Practices for the Family at Home

- Never leave keys hidden outside the home, e.g., under the doormat, flower pot or on top of the door frame.
- If necessary, leave an extra set of house keys with a trusted neighbor or colleague.
- Always keep doors and windows locked, even when you and family members are at home.
- Develop a rapport with your neighbors and offer to keep an eye on each other's property, especially during trips.
- Enter and exit your vehicle inside a closed garage if possible.
- Know where all family members are at all times.

Physical Security of Your Residence

Perimeter

- Keep shrubbery low and not too dense around doors and windows.
- Do not place names on mailboxes or display them on the outside of your home.
- Have locks installed on your fuse box and external power source if located in a common area of a multi-family home.
- If you have a privacy fence around your property, make sure it has a secure locking mechanism.
- Install adequate lighting outside every entryway; consider installing motion sensors and/or automatic timers.

Exterior Doors

- Install quality locks, preferably deadbolts on all exterior doors; garage doors should have either automatic openers or slide bolt locks.
- Never leave your garage door open or unlocked when the garage is unattended.
- Install a wide-angle lens viewer in the front door; never open the door without knowing who is there.
- Do not install "doggy doors," as they make it easier for small intruders to enter your home.

Interior

- Consider installing a home alarm system for additional protection. If you do install a home alarm system, USE IT.
- Keep flashlights in several areas in the house; periodically check them to ensure they function properly.
- Periodically check smoke detectors and change batteries, as necessary.
- Keep at least one fire extinguisher on each floor, especially in the kitchen and garage.

Telephone Security

- Maintain unlisted/unpublished telephone numbers for all family members.
- Post emergency telephone numbers for the local police and fire departments and hospitals in a conspicuous place near the telephone.
- Cellular telephones are desirable and essential for emergency communications in the event of severed telephone lines or power failures. Leave the cellular telephone "on" and near you at night while sleeping.

Domestic Employees

- Thoroughly check the references of all service employees being considered for employment in the home.
- Inform employees of security responsibilities and who to notify in an emergency.

While You are Away

When you are going to be away from home for more than a couple days at a time, the following is recommended:

- notify the local police department and leave emergency contact number with them;
- leave contact numbers and an itinerary with a trusted neighbor or colleague in case of emergency;
- arrange with the U.S. Postal Service to hold all mail;
- make arrangements to have all newspaper deliveries halted until your return;
- set interior and exterior lights, radio and television timers;
- have a trusted neighbor or colleague check the house for flyers, newspapers or other items that may indicate you are away; and
- make arrangements to have the yard mowed or snow removed, as appropriate.

Suspicious Mail or Packages (at home or work)

It is best to avoid acceptance of unordered deliveries, packages or services. Characteristics of suspicious mail or packages include:

- no return address, or has an unusual origin;
- restrictive markings such as "personal";
- sealed with excessive tape;
- address contains misspelled words or are poorly written;
- contains excessive postage;
- wires or strings are protruding;
- envelope/package is rigid or bulky;
- envelope/package has a strange odor;
- envelope/package contains oily residue, stains, crystallization or discoloration; and/or
- envelope/package has an abnormal size, weight or shape.

Do not touch or move a suspicious letter or package and notify local police or FPS immediately.

Additional information and publications regarding suspicious mail can be obtained at the U.S. Postal Inspection Service Web site at www.usps.com/postalinspectors.

Travel Security

Criminal acts against public officials and private citizens usually occur away from your home or workplace since extra security precautions and countermeasures are in place at those locations. It is important to vary your routes of travel and be cautious of establishing routines as you go about your day-to-day schedule.

Vehicle Precautions

- Keep the vehicle in good mechanical condition.
- Do not let the gas tank get too low.
- Install a vehicle alarm to discourage tampering or use a steering wheel lock.
- Never leave the trunk key or other keys with a parking attendant or a maintenance service person (unless needed).
- Always lock your car and avoid parking on the street overnight.
- Do not leave windows down.
- Use a remote garage door opener if available.

On the Street

- Whenever possible, travel with a friend or group.
- Be alert to your surroundings and the people around you, especially if you are traveling alone.
- Stay in well-lit areas as much as possible.
- Walk close to the curb; avoid doorways, bushes and alleys where someone could hide.
- Walk confidently and at a steady pace. Avoid the appearance of being lost.
- Review mental preparations for what you would do were an attack to take place.
- If you are confronted, don't fight back; give up your valuables. Your money and passport can be replaced, but your life cannot.

Traveling by Car

- Know your route and the locations of secure places along that route.
- Inspect your vehicle carefully before entering. Look for evidence of tampering.
- Visually check the hood latch, exhaust pipe, trunk latch, wheel wells, tires, gas cap and the underside of the car.
- Never pick up hitchhikers.
- If the car breaks down, raise the hood and tie a white cloth to the door handle.
- Remain inside with doors locked, if someone stops to offer assistance, ask them to call for help.
- Be alert to possible surveillance. If you suspect you are being followed, go to the nearest secure public place (preferably a police station).
- Have a cell phone with you at all times; ensure that the cell phone is properly charged.
- Communicate frequently, letting others know your location, destination and when you are expected to arrive.
- Avoid driving in the far right-hand lane when possible to prevent being forced over.
- If you see a suspicious roadblock or detour, take an alternate route.

Traveling by Taxi, Train or Bus

- Vary your mode of transportation.
- Try to travel with a companion.
- Don't always use the same taxi company and only take taxis clearly identified with official markings.
- Don't let someone you don't know direct you to a specific taxi.
- If possible, specify the route you want a taxi to follow, and ensure the driver follows any directions you give.
- Ensure the face of the cab driver and the picture on the license are the same.
- Be aware of suspicious or unattended packages.
- Report suspicious behavior or behavior that is not consistent with that of others and notify police or security personnel.

Traveling by Air

- Restrict travel plans to a need-to-know basis.
- Keep your itinerary and travel documents locked in a safe place until needed.
- Provide a copy of your itinerary to your family and your office. Call in from time to time.
- Be aware of nervous behavior or behavior that is not consistent with that of others and notify airport police or a flight attendant.
- If possible, never leave your luggage unattended.
- Don't use official title or office address on tickets, hotel reservations or other travel documents.
- Travel as light as possible; this will allow you to move more quickly and have a free hand available, if needed.
- If you have both civilian and official passports, keep the official one in checked luggage, memorize the passport number and use the civilian one at hotels or other places that request identification.
- Keep medicines in their original, labeled containers. Bring copies of prescriptions and the generic names of drugs.
- Bring traveler's checks and one or two credit cards instead of cash.
- Remain friendly, but be cautious about discussing personal matters, your itinerary or program.

Hotel Precautions

- Keep your room key with you at all times.
- Do not give your room number to anyone you do not know well. Meet visitors in the lobby.
- Keep your room neat and orderly, so you'll recognize if something is out of place when you come back.
- Know the locations of fire exits and plan an exit strategy in case of emergency.
- Do not invite strangers to your room.
- If you must call room service, confirm when they will be arriving and ask for identification upon opening the door.
- Know the telephone number and location of hotel security.
- Do not leave money and other valuables in your hotel room while you are out. Use the hotel safe.
- If you are alone, do not get on an elevator if there is a suspicious-looking person inside.

Terrorist Acts Precautions

Due to the nature of terrorist attacks, it is difficult to protect yourself absolutely. Generally, you should educate yourself about your destination to determine the rates of kidnappings and terrorist acts. If your destination has high rates of these activities, you should reconsider your travel plans. If you do continue with your travel plans, there are some proactive measures you can take to avoid victimization:

- schedule direct flights if possible and avoid stops in high-risk airports or areas;
- as much as possible, avoid luggage tags, dress and behavior that may identify you as an American;
- keep an eye out for suspicious abandoned packages or briefcases. Report them to airport security or other authorities and leave the area promptly;
- avoid obvious terrorist targets such as places where Americans and westerners are known to congregate;
- formulate a plan of action in the event of an attack or other emergency;
- register with the nearest U.S. embassy or consulate through the State Department's travel registration Web site: https://travelregistration.state.gov/ibrs;
- check for loose wires or other suspicious activity around your car;
- drive with car windows closed in crowded streets; bombs can be thrown through open windows.

If you are ever in a situation where somebody starts shooting, drop to the floor or get down as low as possible and try to shield yourself under a solid object. Don't move until you are sure the danger has passed. Do not attempt to help rescuers and do not pick up a weapon as security personnel and responders may not recognize you from the attackers.

U.S. Immigration and Customs Enforcement

Report Suspicious Activity to FPS:

1-877-4FPS-411

(1-877-437-7411)

www.ice.gov

11/2007