FPS

Page 1
Message from the Director
2008 Security Resolutions

Page 2
Feature
Protect Yourself and Your Information

Page 3
FPS In Action
FPS Link
Inside FPS
Improve Performance Through Technology

Page 4
Inside FPS, *continued*
News and Updates
FAQs

News, Information and Updates from the Federal Protective Service • January 2008

The Federal Protective Service

Secure Facilities, Safe Occupants

Protecting the critical infrastructure and key resources of the United States is essential to our nation's security, public health and safety, economic vitality and way of life.

The Federal Protective Service (FPS) protects one component of the nation's infrastructure by mitigating risk to federal facilities and their occupants. We organize our activities along three guiding principles:

- Principle I: Stakeholder Service
- Principle II: Technical Expertise
- Principle III: Organizational Excellence

Report Suspicious Activity to an FPS MegaCenter:

1-877-4FPS-411

(1-877-437-7411)

www.ice.gov

U.S. Immigration and Customs Enforcement

Mr. Gary W. Schenkel

Message from the Director

Resolve to Focus on Security in 2008

The start of a new year is an excellent time to review security procedures in your office and at your facility to ensure that your people, your property and your information are protected. Resolve to make security a top priority this year by encouraging risk reduction and awareness of threats.

In this issue of the FPS newsletter, we share some helpful tips for ways that you can keep yourself and your office safe and secure. By being prepared to recognize suspicious activity, taking simple steps to secure offices and property, and avoiding potentially threatening situations, you can help to reduce the risk to you, your co-workers and your family.

In addition, we share some basic tips on information security and protecting yourself against identity theft. The fact is that we live and work in an increasingly networked world where information management and cyber security have become increasingly important to the FPS mission.

Finally, we are pleased to share some of our recent successes and plans for the coming year:

- The "FPS In Action" section of this issue highlights FPS Link, a Web-based initiative for information sharing efforts that is enhancing FPS' mission effectiveness.
- The "Inside FPS" section focuses on FPS efforts to reduce risk through the FPS Risk Assessment and Management Program (RAMP), a new program we are developing to provide enhanced information to our personnel and to improve service to our stakeholders.

On behalf of all of us at FPS, we wish you and your families a happy and healthy new year. We look forward to continuing to work with you to mitigate risk to federal facilities. Please e-mail us with your input at **FPSInfo@dhs.gov**.

Feature

Protect Yourself and Your Information

With the kick-off of another new year, now is the time to review security policies with your personnel. One of the most important things to remember is that many burglaries, robberies, assaults and other threats can be prevented by basic preparation and alertness. Here are some tips for mitigating risk and preventing potential criminal activity.

Recognize Suspicious Persons

- Challenge wandering or "lost" visitors walking the halls and escort them to the right office or to a "house phone" to call their intended contact.
- Watch out for people who open the wrong doors and pretend to be looking for a specific office or person—they may be attempting to assess vulnerabilities in the building for later criminal activity. If they act nervous or head immediately for the nearest exit, remember their description and call security.
- Arrange office space so that unescorted visitors can be easily noticed. Have staff follow strict access control procedures. Do not allow exceptions.
- Report suspicious people or activity to authorities immediately.

Secure Property

- Lock all doors, windows, drawers, cabinets and conference rooms or storage rooms that are regularly unoccupied or unmonitored.
- Do not leave laptop computers, keys, money, checks or valuables of any kind out in plain view, in unsecured areas, or in unattended jacket or coat pockets.
- Do not leave packages near doorways, on desks or in lobbies, conference rooms, break rooms, cafeterias, rest rooms or other public areas.
- Keep publicly accessible restroom doors locked and set up a key control system. If there is a combination lock, only office personnel should open the lock for visitors.

Protect Yourself

- Stay alert and aware of your surroundings, whether on the street, in an office building or shopping mall, driving, or waiting for public transportation.
- Avoid lightly traveled stairwells and other isolated areas.
- Observe elevator interiors before entering. Avoid riding the elevator alone with a suspicious person. Wait until the next elevator if you are uncertain of any occupant.

- Send a message that you are calm, confident and know where you are going.

Prevent Individual Identify Theft

- Do not give out personal information over the phone, through the mail, or over the Internet unless you have initiated the contact or know who you are dealing with.
- Shred all documents, including pre-approved credit applications received in your name, insurance forms, bank checks and statements you are discarding, and other financial information.
- Do not use your mother's maiden name, your birth date, the last four digits of your Social Security number, or a similar series of numbers as a password for anything.
- Carry only the identification information and the number of credit and debit cards that you need.

If you would like to learn more about crime prevention and awareness, FPS provides training in these critical areas to tenants of facilities managed by the General Services Administration. These training programs are customized to meet the needs of your facility to ensure appropriate content for the risks and threats you and your co-workers may face.

Contact your facility's Building Security Committee or your regional FPS representative for more information.

FPS In Action

FPS Link—Connecting Law Enforcement

With responsibility for approximately 9,000 federal facilities nationwide, FPS personnel protect more than one million people who work in and visit the nation's federal offices, courthouses and other facilities every day. That is a big responsibility, and it means that sharing information among law enforcement agencies is critical to mitigate risk and to ensure timely response when a threat emerges.

In order to ensure comprehensive preparedness and coordinate response for facilities, FPS works in concert with other law enforcement agencies.

The FPS Link program is one example of how that information is conveyed quickly and efficiently via the Internet. Former FPS Special Agent Bill Bonk, a career federal criminal investigator, created FPS Link in 2004 as a Web-based solution to connect local law enforcement personnel with FPS to share information in real time, 24 hours a day.

According to Bonk, who now serves as administrator of FPS Link, the real-time, round-the-clock accessibility of the Web site is what makes it unique among information sharing portals.

"Responders can log on to FPS Link at any time, from any location, and with any device that has Internet access," he said. "The information they post here helps others make informed decisions about what needs to happen next. Timeliness and consistency are critical."

FPS Link currently hosts approximately 4,000 members, including state and local government fusion centers, law enforcement operations centers, the intelligence community, and emergency operations or watch centers for federal departments and agencies that occupy government owned or leased property.

Bonk and his team gather information from FPS Link users; the National Law Enforcement Telecommunications System; federal, state and local law enforcement; operations centers; other online portals; and even open sources. This information is then posted and shared with the community. All information is unclassified (including For Official Use Only and Law Enforcement Sensitive) and most relates to protection of federal infrastructure or government operations, as well as officer safety.

Access to the FPS Link Web site requires a user name and password for log-in and is limited to law enforcement personnel or approved government employees. For more information, including how to find out if you are eligible for access to the site, send an e-mail request to **FPSInfo@dhs.gov**.

Inside FPS

Improving Performance through Technology

FPS is embarking on a program to develop state-of-the-art tools to support risk mitigation at federal facilities. The FPS Risk Assessment and Management Program (RAMP) is a new tool being developed to replace existing systems used to assess risk, track countermeasures and measure their effectiveness.

continued on page 4

Participants of the RAMP workshop held for FPS inspectors.

Participants of the RAMP workshop held for FPS managers, including area commanders and law enforcement program managers.

Inside FPS

continued from page 3

Using input received from FPS inspectors and area commanders during two workshops held in 2007, this system will improve FPS' ability to collect, store, analyze and report on the information needed to effectively manage risk. Future issues of this newsletter will detail the RAMP tool more fully as the program is developed and implemented.

News and Updates

Ensuring FPS customers understand the service they are receiving is one of many steps the organization is taking to enhance communication and information sharing with stakeholders. In the last quarter, FPS developed and distributed a new *Security Services and Pricing Provisions* document that explains the basic security charges that are billed by FPS to all tenants in GSA-controlled space.

Security services provided for GSA-controlled facilities, as promulgated in 41 CFR 102-85.35 and further defined in a memorandum of agreement between FPS and GSA, include the following:

- general law enforcement on property controlled by the GSA's Public Buildings Service;
- physical security assessments;
- crime prevention and awareness training;
- advice and assistance to building security committees;
- intelligence sharing;
- criminal investigation;
- assistance and coordination in developing Occupant Emergency Plans;
- coordinating mobilization and response to terrorist threats or civil disturbances;
- program administration for security guard contracts; and
- MegaCenter operations for monitoring building perimeter alarms and dispatching appropriate law enforcement response.

For more information on these efforts, or to request a copy of the *Security Services and Pricing Provisions* document, please e-mail FPS at **FPSInfo@dhs.gov**.

FAQs

We received the following question in response to our release of the Occupant Emergency Plan (OEP) Guide, which includes a template format for emergency managers and planners to use in developing OEPs for their facilities.

Are facility emergency coordinators and designated officials required to follow this new format? If not, are they required to incorporate the considerations and content into a facility (agency)-specific format that matches the OEP Guide provided by FPS?

Facility emergency coordinators and designated officials are not required to use the new format when creating a facility OEP, but it is highly recommended. FPS has refined this format to ensure federal facilities are presented with a consistent format to use for planning purposes. A consistent and nationally coordinated structure for response to emergency situations will lead to more comprehensive preparedness. As such, FPS has worked to create an overall guidance document in a universal template format that individual facilities can customize with information relevant to its protection needs.