United States Government Accountability Office

GAO

Testimony

Before the House Committee on Homeland Security

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, November 18, 2009

HOMELAND SECURITY

Greater Attention to Key Practices Would Help Address Security Vulnerabilities at Federal Buildings

Statement of Mark L. Goldstein, Director
Physical Infrastructure Issues

November 18, 2009

HOMELAND SECURITY

Greater Attention to Key Practices Would Help Address Security Vulnerabilities at Federal Buildings

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-236T, a testimony to the Chairman, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The Federal Protective Service (FPS) within the Department of Homeland Security (DHS) is responsible for providing law enforcement and related security services for nearly 9,000 federal facilities under the control and custody of the General Services Administration (GSA). In 2004 GAO identified a set of key protection practices from the collective practices of federal agencies and the private sector, which included allocation of resources using risk management, strategic management of human capital, leveraging of technology, information sharing and coordination, and performance measurement and testing.

This testimony is based on past reports and testimonies and discusses (1) limitations FPS faces in protecting GSA buildings and resulting vulnerabilities; and (2) actions FPS is taking. To perform this work, GAO used its key practices as criteria, visited a number of GSA buildings, surveyed tenant agencies, analyzed pertinent laws and DHS and GSA documents, conducted covert testing at 10 judgmentally selected high-security buildings in four cities, and interviewed officials from DHS, GSA, and tenant agencies, and contractors and guards.

What GAO Recommends

GAO makes no new recommendations in this testimony. DHS concurred with GAO's past recommendations for FPS, but FPS has not completed many related corrective actions.

View GAO-10-236T or key components. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

FPS's approach to securing GSA buildings reflects some aspects of key protection practices; however, GAO found limitations in each area and identified vulnerabilities. More specifically:

- FPS faces obstacles in *allocating resources using risk management*. FPS uses an outdated risk assessment tool and a subjective, time-consuming process to assess risk. In addition, resource allocation decisions are the responsibility of GSA and tenant agencies. This leads to uncertainty about whether risks are being mitigated. Also, FPS continues to struggle with funding challenges that impede its ability to allocate resources effectively.

- FPS does not have a *strategic human capital management* plan to guide its current and future workforce planning efforts, making it difficult to discern how effective its transition to an inspector-based workforce will be. Furthermore, because contract guards were not properly trained and did not comply with post orders, GAO investigators concealing components for an improvised explosive device passed undetected by FPS guards at 10 of 10 high-security facilities in four major cities.

- FPS lacks a systematic approach for *leveraging technology*, and inspectors do not provide tenant agencies with an analysis of alternative technologies, their cost, and the associated reduction in risk. As a result, there is limited assurance that the recommendations inspectors make are the best available alternatives, and tenant agencies must make resource allocation decisions without key information.

- FPS has developed *information sharing and coordination* mechanisms with GSA and tenant agencies, but there is inconsistency in the type of information shared and the frequency of coordination.

- FPS lacks a reliable data management system for accurately tracking *performance measurement and testing*. Without such a system, it is difficult for FPS to evaluate and improve the effectiveness of its efforts, allocate resources, or make informed risk management decisions.

FPS is taking some steps to better protect GSA buildings. For example, FPS is developing a new risk assessment program and has recently focused on improving oversight of its contract guard program. Additionally, GAO has recommended that FPS implement specific actions to make greater use of key practices and otherwise improve security. However, FPS has not completed many related corrective actions and FPS faces implementation challenges as well. Nonetheless, adhering to key practices and implementing GAO's recommendations in specific areas would enhance FPS's chances for future success, and could position FPS to become a leader and benchmark agency for facility protection in the federal government.

Mr. Chairman and Members of the Committee:

We are pleased to be here to discuss the Federal Protective Service's (FPS) efforts to ensure the protection of the more than 1 million government employees, as well as members of the public, who work in and visit the nearly 9,000 federal facilities that are under the control and custody of the General Services Administration (GSA). There has not been a large-scale attack on a domestic federal facility since the terrorist attacks of September 11, 2001, and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Nevertheless, the shooting death this past year of a guard at the U.S. Holocaust Memorial Museum—though not a federal facility—demonstrates the continued vulnerability of public buildings. Moreover, the challenge of protecting federal real property is one of the major reasons for GAO's designation of federal real property management as a high-risk area.[1]

FPS—within the Department of Homeland Security (DHS)—is authorized to protect the buildings, grounds, and property that are under the control and custody of GSA, as well as the persons on the property; to enforce federal laws and regulations aimed at protecting GSA buildings and persons on the property; and to investigate offenses against these buildings and persons.[2] FPS conducts its mission by providing security services through two types of activities: (1) physical security activities—conducting building risk assessments of facilities and recommending countermeasures aimed at preventing incidents at facilities—and (2) law enforcement activities—proactively patrolling facilities, responding to incidents, conducting criminal investigations, and exercising arrest authority. To accomplish its mission of protecting federal facilities, FPS currently has a budget[3] of around $1 billion, nearly 1,200 full time employees, and about 15,000 contract security guards deployed at federal facilities across the country.

We have identified a set of key facility protection practices from the collective practices of federal agencies and the private sector to provide a

[1]GAO, *High Risk Series: An Update*, GAO-09-271 (Washington, D.C.: Jan. 1, 2009).

[2]40 U.S.C. § 1315.

[3]Funding for FPS is provided through revenues and collections of security fees charged to building tenants in FPS-protected property. The revenues and collections are credited to FPS's appropriation and are available until expended for the protection of federally owned and leased buildings and for FPS's operations.

framework for guiding agencies' protection efforts and addressing challenges.[4] The key practices essentially form the foundation of a comprehensive approach to building protection. We have used these key practices to evaluate how FPS protects GSA buildings and will focus on the following five key practices for this testimony:[5]

- *Allocation of resources using risk management.* Identify threats, assess vulnerabilities, and determine critical assets to protect, and use information on these and other elements to develop countermeasures and prioritize the allocation of resources as conditions change.
- *Strategic management of human capital.* Manage human capital to maximize government performance and ensure accountability in asset protection through, for example, recruitment of skilled staff, training, and retention.
- *Leveraging of technology.* Select technologies to enhance asset security through methods like access control, detection, and surveillance systems. This involves not only using technology, but also ensuring positive returns on investments in the form of reduced vulnerabilities.
- *Information sharing and coordination.* Establish means of coordinating and sharing security and threat information internally, within large organizations, and externally, with other government entities and the private sector.
- *Performance measurement and testing.* Use metrics, such as implementation timelines, and active testing, such as unannounced on-site assessments, to ensure accountability for achieving program goals and improving security at facilities.

[4]GAO, *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices*, GAO-05-49 (Washington, D.C.: Nov. 30, 2004).

[5]We did not include the key practice of aligning assets to mission because GSA, not FPS, controls the asset inventory.

This testimony is based on past reports and testimonies[6] and discusses (1) limitations FPS faces in protecting GSA buildings and resulting vulnerabilities and (2) actions FPS is taking to address challenges. Work for these past reports and testimonies included using our key practices as a framework for assessing facility protection efforts by FPS management and at individual buildings. We also visited FPS regions and selected GSA buildings to assess FPS activities firsthand. We surveyed a sample of 1,398 federal officials who work in GSA buildings in FPS's 11 regions and are responsible for collaborating with FPS on security issues. Additionally, we reviewed training and certification data for 663 randomly selected guards in 6 of FPS's 11 regions. Because of the sensitivity of some of the information in our prior work, we cannot specifically identify the locations of the incidents discussed. We also conducted covert testing at 10 judgmentally selected high-risk facilities in four cities. For all of our work, we reviewed related laws and directives, interviewed officials and analyzed documents and data from DHS and GSA, and interviewed tenant agency representatives, contractors, and guards. The previous work on which this testimony is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[6]This testimony draws upon five primary sources. We reported on FPS's allocation of resources using risk management, leveraging of technology, and information sharing and coordination in GAO, *Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection*, GAO-10-142 (Washington, D.C.: Oct. 23, 2009). We reported on FPS's strategic management of human capital in GAO, *Homeland Security: Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist*, GAO-09-1047T (Washington, D.C.: Sept. 23, 2009); GAO, *Homeland Security: Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered By Weaknesses in Its Contract Security Guard Program*, GAO-09-859T (Washington, D.C.: July 8, 2009); and GAO, *Homeland Security: Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants*, GAO-09-749 (Washington, D.C.: July 30, 2009). We reported on FPS's performance measurement and testing in GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities*, GAO-08-683 (Washington, D.C.: June 11, 2008).

FPS Faces Challenges in Many Areas, Raising Concerns about Vulnerabilities

Risk Management Approach Is Inadequate and Has Limitations

FPS assesses risk and recommends countermeasures to GSA and tenant agencies; however, FPS's ability to influence the allocation of resources using risk management is limited because resource allocation decisions are the responsibility of GSA and tenant agencies, which may be unwilling to fund the countermeasures FPS recommends. We have found that under the current risk management approach, the security equipment that FPS recommends and is responsible for acquiring, installing, and maintaining may not be implemented if tenant agencies are unwilling to fund it.[7] For example, in August 2007 FPS recommended a security equipment countermeasure—the upgrade of a surveillance system shared by two high-security locations that, according to FPS officials, would cost around $650,000. While members of one building security committee (BSC) told us they approved spending between $350,000 and $375,000 to fund their agencies' share of the countermeasure, they said that the BSC of the other location would not approve funding; therefore, FPS could not upgrade the system it had recommended. In November 2008 FPS officials told us that they were moving ahead with the project by drawing on unexpended revenues from the two locations' building-specific fees and the funding that was approved by one of the BSCs. Furthermore, FPS officials, in May 2009, told us that all cameras had been repaired and all monitoring and recording devices had been replaced, and that the two BSCs had approved additional upgrades and that FPS was implementing them. As we reported in June 2008, we have found other instances in which recommended security countermeasures were not implemented at some of the buildings we visited because BSC members could not agree on which countermeasures to implement or were unable to obtain funding from their agencies.[8]

Compounding this situation, FPS takes a building-by-building approach to risk management, using an outdated risk assessment tool to create building security assessments (BSA), rather than taking a more

[7] GAO-10-142.

[8] GAO-08-683.

comprehensive, strategic approach and assessing risks among all buildings in GSA's inventory and recommending countermeasure priorities to GSA and tenant agencies. As a result, the current approach provides less assurance that the most critical risks at federal buildings across the country are being prioritized and mitigated. Also, GSA and tenant agencies have concerns about the quality and timeliness of FPS's risk assessment services and are taking steps to obtain their own risk assessments. For example, GSA officials told us they have had difficulties receiving timely risk assessments from FPS for space GSA is considering leasing. These risk assessments must be completed before GSA can take possession of the property and lease it to tenant agencies. An inefficient risk assessment process for new lease projects can add costs for GSA and create problems for both GSA and tenant agencies that have been planning for a move. Therefore, GSA is updating a risk assessment tool that it began developing in 1998, but has not recently used, to better ensure the timeliness and comprehensiveness of these risk assessments. GSA officials told us that in the future they may use this tool for other physical security activities, such as conducting other types of risk assessments and determining security countermeasures for new facilities. Additionally, although tenant agencies have typically taken responsibility for assessing risk and securing the interior of their buildings, assessing exterior risks will require additional expertise and resources. This is an inefficient approach considering that tenant agencies are paying FPS to assess building security.

Finally, FPS continues to struggle with funding challenges that impede its ability to allocate resources to more effectively manage risk. FPS faces challenges in ensuring that its fee-based funding structure accounts for the varying levels of risk and types of services provided at federal facilities. FPS funds its operations through security fees charged to tenant agencies. However, FPS's basic security fee, which funds most of its operations, does not account for the risk faced by specific buildings, the level of service provided, or the cost of providing services, raising questions about equity.[9] FPS charges federal agencies the same basic security fee regardless of the perceived threat to a particular building or agency. In fiscal year 2009, FPS charged 66 cents per square foot for basic security. Although FPS categorizes buildings according to security levels based on its assessment of each building's risk and size, this assessment does not

[9]Some of the basic security services covered by this fee include law enforcement activities at GSA facilities, preliminary investigations, the capture and detention of suspects, and completion of BSAs.

affect the security fee FPS charges. For example, level I facilities typically face less risk because they are generally small storefront-type operations with a low level of public contact, such as a Social Security Administration office. However, these facilities are charged the same basic security fee of 66 cents per square foot as a level IV facility that has a high volume of public contact and may contain high-risk law enforcement and intelligence agencies and highly sensitive government records. We also have reported that basing government fees on the cost of providing a service promotes equity, especially when the cost of providing the service differs significantly among different users, as is the case with FPS. In our June 2008 report, we recommended that FPS improve its use of the fee-based system by developing a method to accurately account for the cost of providing security services to tenant agencies and ensuring that its fee structure takes into consideration the varying levels of risk and service provided at GSA facilities.[10] We also recommended an evaluation of whether FPS's current use of a fee-based system or an alternative funding mechanism is the most appropriate manner to fund the agency. While DHS agreed with these recommendations, FPS has not fully implemented them.

Improvements Needed in Human Capital Planning and Contract Guard Management

FPS does not have a strategic human capital plan to guide its current and future workforce planning efforts, including effective processes for training, retention, and staff development. Instead, FPS has developed a short-term hiring plan that does not include key human capital principles, such as determining an agency's optimum staffing needs. Moreover, FPS has been transitioning to an inspector-based workforce, thus eliminating the police officer position and relying primarily on FPS inspectors for both law enforcement and physical security activities. FPS believes that this change will ensure that its staff has the right mix of technical skills and training needed to accomplish its mission. However, FPS's ability to provide law enforcement services under its inspector-based workforce approach may be diminished because FPS will rely on its inspectors to provide these services and physical security services simultaneously. In the absence of a strategic human capital plan, it is difficult to discern how effective an inspector-based workforce approach will be. The lack of a human capital plan has also contributed to inconsistent approaches in how FPS regions and headquarters are managing human capital activities. For example, FPS officials in some of the regions we visited said they implement their own procedures for managing their workforce, including

[10] GAO-08-683.

processes for performance feedback, training, and mentoring. Additionally, FPS does not collect data on its workforce's knowledge, skills, and abilities. These elements are necessary for successful workforce planning activities, such as identifying and filling skill gaps and succession planning. We recently recommended that FPS improve how it collects data on its workforce's knowledge, skills, and abilities to help it better manage and understand current and future workforce needs; and use these data in the development and implementation of a long-term strategic human capital plan that addresses key principles for effective strategic workforce planning.[11] DHS concurred with our recommendations.

Furthermore, FPS did not meet its fiscal year 2008 mandated deadline of increasing its staffing level to no fewer than 1,200 full-time employees by July 31, 2008, and instead met this staffing level in April 2009.[12] FPS's staff has steadily declined since 2004 and critical law enforcement services have been reduced or eliminated. For example, FPS has eliminated its use of proactive patrol to prevent or detect criminal violations at many GSA buildings. According to some FPS officials at regions we visited, not providing proactive patrol has limited its law enforcement personnel to a reactive force.[13] Additionally, officials stated that in the past, proactive patrol permitted its police officers and inspectors to identify and apprehend individuals that were surveilling GSA buildings. In contrast, when FPS is not able to patrol federal buildings, there is increased potential for illegal entry and other criminal activity. In one city we visited, a deceased individual had been found in a vacant GSA facility that was not regularly patrolled by FPS. FPS officials stated that the deceased individual had been inside the building for approximately 3 months.

FPS does not fully ensure that its contract security guards have the training and certifications required to be deployed to a GSA building.[14] We have noted that the effectiveness of a risk management approach depends

[11]GAO-09-749.

[12]This mandate in DHS's fiscal year 2008 was effective for fiscal year 2008 only, since mandates in annual appropriation acts are presumed to be applicable for that fiscal year unless specified to the contrary. DHS's appropriation act for fiscal year 2009 also mandated that FPS have no fewer than 1,200 full-time employees. See Pub. L. No. 110-161, Div. E, 121 Stat. 1844, 2051-2052 (2007) and Pub. L. No. 110-329, Div. D, 122 Stat. 3574, 3659-3660 (2008).

[13]GAO-08-683.

[14]GAO-09-859T.

on the involvement of experienced and professional security personnel.[15] Further, that the chances of omitting major steps in the risk management process increase if personnel are not well trained in applying risk management. FPS requires that all prospective guards complete about 128 hours of training including 8 hours of X-ray and magnetometer training. However, in one region, FPS has not provided the X-ray or magnetometer training to its 1,500 guards since 2004. Nonetheless, these guards are assigned to posts at GSA buildings. X-ray training is critical because guards control access points at buildings. Insufficient X-ray and magnetometer training may have contributed to several incidents at GSA buildings in which guards were negligent in carrying out their responsibilities. For example, at a level IV[16] federal facility in a major metropolitan area, an infant in a carrier was sent through an X-ray machine due to a guard's negligence.[17] Specifically, according to an FPS official in that region, a woman with her infant in a carrier attempted to enter the facility, which has child care services. While retrieving her identification, the woman placed the carrier on the X-ray machine. Because the guard was not paying attention and the machine's safety features had been disabled,[18] the infant in the carrier was sent through the X-ray machine. FPS investigated the incident and dismissed the guard; however, the guard subsequently sued FPS for not providing the required X-ray training. The guard won the suit because FPS could not produce any documentation to show that the guard had received the training, according to an FPS official. In addition, FPS officials from that region could not tell us whether the X-ray machine's safety features had been repaired. Additionally, we found that FPS does not have a fully reliable system for monitoring and verifying guard training and certification requirements. We reviewed 663 randomly selected guard records and found that 62 percent of the guards had at least one expired certification, including a declaration that guards have not been convicted of domestic violence, which make them ineligible to carry firearms.

[15]GAO-05-49.

[16]At the time of our review, a level IV facility had more than 450 federal employees, more than 150,000 square feet, a high volume of public contact, and tenant agencies that could include high-risk law enforcement and intelligence agencies, courts, judicial offices, and highly sensitive government records.

[17]X-ray machines are hazardous because of the potential radiation exposure. In contrast, magnetometers do not emit radiation and are used to detect metal.

[18]With this safety feature disabled, the X-ray machine's belt was operating continuously although the guard was not present.

We also found that some guards were not provided building-specific training, such as what actions to take during a building evacuation or a building emergency.[19] This lack of training may have contributed to several incidents where guards neglected their assigned responsibilities. For example,

- at a level IV facility, the guards did not follow evacuation procedures and left two access points unattended, thereby leaving the facility vulnerable;
- at a level IV facility, the guard allowed employees to enter the building while an incident involving suspicious packages was being investigated; and,
- at a level III facility,[20] the guard allowed employees to access the area affected by a suspicious package, which was required to be evacuated.

FPS has limited assurance that its guards are complying with post orders.[21] It does not have specific national guidance on when and how guard inspections should be performed. FPS's inspections of guard posts at GSA buildings are inconsistent and the quality varied in the six regions we examined. We also found that guard inspections are typically completed by FPS during regular business hours and in locations where FPS has a field office, and seldom on nights or weekends. However, on an occasion when FPS officials conducted a post inspection at night, they found a guard asleep at his post after taking a pain-killer prescription drug. FPS also found other incidents at high-security facilities where guards neglected or inadequately performed their assigned responsibilities. For example, a guard failed to recognize or did not properly X-ray a box containing handguns at the loading dock at a facility. FPS became aware of the situation because the handguns were delivered to FPS.

Because guards were not properly trained and did not comply with post orders, our investigators—with the components for an improvised explosive device (IED) concealed on their persons—passed undetected through access points controlled by FPS guards at 10 of 10 level IV

[19]GAO-09-859T.

[20]At the time of our review, a level III facility had between 151 and 450 federal employees, 80,000 to 150,000 square feet, and a moderate to high volume of public contact.

[21]GAO-09-859T.

facilities in four major cities where GAO conducted covert tests.[22] The specific components for this device, items used to conceal the device components, and the methods of concealment that we used during our covert testing are classified, and thus are not discussed in this testimony. Of the 10 level IV facilities our investigators penetrated, 8 were government owned and 2 were leased facilities. The facilities included district offices of a U.S Senator and a U.S. Representative as well as agencies of the Departments of Homeland Security, Transportation, Health and Human Services, Justice, State, and others. The two leased facilities did not have any guards at the access control points at the time of our testing. Using publicly available information, our investigators identified a type of device that a terrorist could use to cause damage to a federal facility and threaten the safety of federal workers and the general public. The device was an IED made up of two parts—a liquid explosive and a low-yield detonator—and included a variety of materials not typically brought into a federal facility by employees or the public. Although the detonator itself could function as an IED, investigators determined that it could also be used to set off a liquid explosive and cause significantly more damage. To ensure safety during this testing, we took precautions so that the IED would not explode. For example, we lowered the concentration level of the material.[23] To gain entry into each of the 10 level IV facilities, our investigators showed a photo identification (a state driver's license) and walked through the magnetometers without incident. Our investigators also placed their briefcases with the IED material on the conveyor belt of the X-ray machine, but the guards detected nothing. Furthermore, our investigators did not receive any secondary searches from the guards that might have revealed the IED material that they brought into the facilities. At security checkpoints at 3 of the 10 facilities, our investigators noticed that the guard was not looking at the X-ray screen as some of the IED components passed through the machine. A guard questioned an item in the briefcase at one of the 10 facilities but the materials were subsequently allowed through the X-ray machines. At each facility, once past the guard screening checkpoint, our investigators proceeded to a restroom and assembled the IED. At some of the facilities, the restrooms were locked. Our investigators gained access by asking

[22]GAO-09-859T.

[23]Tests that we performed at a national laboratory in February 2006 and July 2007 demonstrated that a terrorist using these devices could cause severe damage to a federal facility and threaten the safety of federal workers and the general public. Our investigators obtained the components for these devices at local stores and over the Internet for less than $150.

employees to let them in. With the IED completely assembled in a briefcase, our investigators walked freely around several floors of the facilities and into various executive and legislative branch offices, as described above.

Systematic Approach for Cost-Effectively Leveraging Technology Is Lacking

Leveraging technology is a key practice over which FPS has somewhat more control, but FPS does not have a comprehensive approach for identifying, acquiring, and assessing the cost-effectiveness of the security equipment that its inspectors recommend. Individual FPS inspectors have considerable latitude in determining which technologies and other countermeasures to recommend, but the inspectors receive little training and guidance in how to assess the relative cost-effectiveness of these technologies or determine the expected return on investment. FPS officials told us that inspectors make technology decisions based on the initial training they receive, personal knowledge and experience, and contacts with vendors. FPS inspectors receive some training in identifying and recommending security technologies as part of their initial FPS physical security training. Since FPS was transferred to DHS in 2003, its refresher training program for inspectors has primarily focused on law enforcement. Consequently, inspectors lack recurring technology training. Additionally, FPS does not provide inspectors with specialized guidance and standards for cost-effectively selecting technology. In the absence of specific guidance, inspectors follow the Department of Justice minimum countermeasure standards[24] and other relevant Interagency Security Committee standards,[25] but these standards do not assist users in selecting cost-effective technologies. Moreover, the document that FPS uses to convey its countermeasure recommendations to GSA and tenant agencies—the BSA executive summary—includes cost estimates but no analysis of alternatives. As a result, GSA and tenant agencies have limited assurance that the investments in technologies and other countermeasures that FPS inspectors recommend are cost-effective, consistent across buildings, and the best available alternatives.

[24]U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C., June 28, 1995). The Department of Justice standards recommend minimum security measures for federal buildings.

[25]Following the Oklahoma City bombing, Executive Order 12977 called for the creation of an interagency security committee to address the quality and effectiveness of physical security requirements for federal facilities by developing and evaluating security standards. The Interagency Security Committee has representation from all major federal departments and agencies.

For example, at one location we visited, an explosives detection dog was used to screen mail that is distributed elsewhere.[26] In 2006, FPS had recommended, based on the results of its risk analysis, the use of this dog and an X-ray machine, although at the time of our visit only the dog was being used. Moreover, the dog and handler work 12-hour shifts Monday through Friday when most mail is delivered and shipped, and the dog needs a break every 7 minutes. The GSA regional security officials[27] we spoke with questioned whether this approach was more effective and efficient than using an on-site enhanced X-ray machine that could detect biological and chemical agents as well as explosives and could be used anytime. In accordance with its policies, FPS conducted a BSA of the site in 2008 and determined that using an enhanced X-ray machine and an explosives detection dog would bring the projected threat rating of the site down from moderate to low. FPS included estimated one-time installation and recurring costs in the BSA and executive summary, but did not include the estimated cost and risk of the following mail screening options: (1) usage of the dog and the additional countermeasure; (2) usage of the additional countermeasure only; and (3) usage of the dog only. Consequently, tenant agency representatives would have to investigate the cost and risk implications of these options on their own to make an informed resource allocation decision.

Information Sharing and Coordination Practices Lack Consistency

It is critical that FPS—as the provider of law enforcement and related security services for GSA buildings—and GSA—as the manager of these properties—have well-established lines of communication with each other and with tenant agencies to ensure that all parties are aware of the ever-changing risks in a dynamic threat environment and that FPS and GSA are taking appropriate actions to reduce vulnerabilities. While FPS and GSA top management have established communication channels, the types of information shared at the regional and building levels are inconsistent, and overall, FPS and GSA disagree over what information should be shared. For example, the memorandum of agreement between DHS and GSA specifies that FPS will provide quarterly briefings at the regional level, but

[26]GAO-10-142.

[27]In 2006 GSA established the Building Security and Policy Division within its Public Buildings Service to oversee its security operations and policies and liaise with FPS. Additionally, the division developed the Regional Security Network, which consists of several staff per GSA region to further enhance coordination with FPS at the regional and building levels, and to carry out GSA security policy in collaboration with FPS and tenant agencies.

FPS had not been providing them consistently across all regions. FPS resumed the practice in October 2008, however, GSA security officials said that these briefings mostly focused on crime statistics and did not constitute comprehensive threat analyses. Additionally, FPS is only required to meet formally with GSA property managers and tenant agencies as part of the BSA process—an event that occurs every 2 to 5 years, depending on a building's security level. We identified information sharing gaps at several level III and IV sites that we visited, and found that in some cases these deficiencies led to decreased security awareness and increased risk.[28]

- At one location, we observed during our interview with the BSC that the committee members were confused about procedures for screening visitors who are passengers in employees' cars that enter the building via the parking garage. One of the tenants recounted an incident in which a security guard directed the visitor to walk through the garage to an appropriate screening station. According to the GSA property manager, this action created a safety hazard. The GSA property manager knew the appropriate screening procedure, but told us there was no written policy on the procedure that members could access. Additionally, BSC members told us that the committee met as needed.

- At one location, FPS had received inaccurate square footage data from GSA and had therefore overcharged the primary tenant agency for a guard post that protected space shared by all the tenants. According to the GSA property manager, once GSA was made aware of the problem, the agency obtained updated information and worked with the tenant agencies to develop a cost-sharing plan for the guard post, which made the primary tenant agency's security expenses somewhat more equitable. BSC members told us that the committee met regularly.

- At one location, members of a BSC told us that they met as needed, although even when they hold meetings, one of the main tenant agencies typically does not participate. GSA officials commented that this tenant adheres to its agency's building security protocols and does not necessarily follow GSA's tenant policies and procedures, which GSA thinks creates security risks for the entire building.

- At one location, tenant agency representatives and officials from FPS told us they met regularly, but GSA officials told us they were not invited to

[28] GAO-10-142.

these meetings. GSA officials at this location told us that they invite FPS to their property management meetings for that location, but FPS does not attend. GSA officials also said they do not receive timely incident information for the site from FPS and suggested that increased communication among the agencies would help them be more effective managers of their properties and provide tenants with better customer service.

- At one location, GSA undertook a major renovation project beginning in April 2007. FPS, GSA, and tenant agency representatives did not all meet together regularly to make security preparations or manage security operations during construction. FPS officials told us they had not been invited to project meetings, although GSA officials told us that they had invited FPS and that FPS attended some meetings. In May 2008, FPS discovered that specific surveillance equipment had been removed. As of May 2009, FPS officials told us they did not know who had removed the equipment and were working with tenant agency representatives to recover it. However, in June 2009 tenant agency representatives told us that they believed FPS was fully aware that the equipment had been removed in December 2007.[29]

Additionally, we conducted a survey of GSA tenant agencies and found that they had mixed views about some of the services they pay FPS to provide.[30] Notably, the survey results indicated that the roles and responsibilities of FPS and tenant agencies are unclear, primarily because on average about one-third of tenant agencies could not comment on how satisfied or dissatisfied they were with FPS's level of communication of its services, partly because they had little to no interaction with FPS officers. Although FPS plans to implement education and outreach initiatives to improve customer service to tenant agencies, it will face challenges because of its lack of complete and accurate contact data. During the course of our review, we found that approximately 53 percent of the e-mail addresses and 27 percent of the telephone numbers for designated points of contacts were missing from FPS's contact database and the database required a substantial amount of revising. Complete and accurate contact information for FPS's customers is critical for information sharing and an

[29]In June 2009 tenant agency representatives told us that at all times, they had been aware of the location of the equipment and assured proper safeguarding of the equipment during the reconstruction process.

[30]GAO-09-749.

essential component of any customer service initiative. Therefore, to improve its services to GSA and tenant agencies, we recommended that FPS collect and maintain an accurate and comprehensive list of all facility-designated points of contact, as well as a system for regularly updating this list; and develop and implement a program for education and outreach to GSA and tenant agencies to ensure they are aware of the current roles, responsibilities, and services provided by FPS.[31] DHS concurred with our recommendations.

Furthermore, while FPS and GSA acknowledge that the two organizations are partners in protecting and securing GSA buildings, FPS and GSA fundamentally disagree over how much of the information in the BSA should be shared. Per the memorandum of agreement, FPS is required to share the BSA executive summary with GSA and FPS believes that this document contains sufficient information for GSA to make decisions about purchasing and implementing FPS's recommended countermeasures. However, GSA officials at all levels cite limitations with the BSA executive summary saying, for example, that it does not contain enough contextual information on threats and vulnerabilities to support FPS's countermeasure recommendations and justify the expenses that GSA and tenant agencies would incur by installing additional countermeasures. Moreover, GSA security officials told us that FPS does not consistently share BSA executive summaries across all regions. Instead, GSA wants to receive BSAs in their entirety so that it can better protect GSA buildings and the tenants who occupy them. According to GSA, building protection functions are an integral part of its property preservation, operation, and management responsibilities.

In a post-September 11th era, it is crucial that federal agencies work together to share information to advance homeland security and critical infrastructure protection efforts. Information is a vital tool in fighting terrorism, and the timely dissemination of that information to the appropriate government agency is absolutely critical to maintaining the security of our nation. The ability to share security-related information can unify the efforts of federal agencies in preventing or minimizing terrorist attacks. However, in the absence of comprehensive information-sharing plans, many aspects of homeland security information sharing can be ineffective and fragmented. In 2005, we designated information sharing for homeland security as a governmentwide high-risk area because of the

[31]GAO-09-749.

significant challenges faced in this area[32]—challenges that are still evident today. It is critical that FPS and GSA—which both have protection functions for GSA buildings, their occupants, and those who visit them—reach consensus on sharing information in a timely manner to support homeland security and critical infrastructure protection efforts.

We recently recommended that FPS reach consensus with GSA on what information contained in the BSA is needed for GSA to fulfill its responsibilities related to the protection of federal buildings and occupants, and accordingly, establish internal controls to ensure that shared information is adequately safeguarded; guidance for employees to use in deciding what information to protect with sensitive but unclassified designations; provisions for training on making designations, controlling, and sharing such information with GSA and other entities; and a review process to evaluate how well this information sharing process is working, with results reported to the Secretary of Homeland Security.[33] While DHS concurred with this recommendation, we are concerned that the steps it described in its response were not comprehensive enough to address the intent of the recommendation. For example, DHS did not explicitly commit to reaching consensus with GSA in identifying building security information that can be shared, or to the steps we outlined in our recommendation—steps that in our view comprise a comprehensive plan for sharing and safeguarding sensitive information. Therefore, it is important that FPS engage GSA in identifying what building security information can be shared and follow the information sharing and safeguarding steps we included in our recommendation to ensure that GSA acquires the information it needs to protect the 9,000 buildings under its control and custody, the federal employees who work in them, and those who visit them.

Performance Measurement Is Limited

We have reported that FPS is limited in its ability to assess the effectiveness of its efforts to protect GSA buildings.[34] To determine how well it is accomplishing its mission to protect GSA buildings, FPS has identified some output measures that are a part of the Office of Management and Budget's Performance Assessment Rating Tool. These measures include determining whether security countermeasures have been deployed and are fully operational, the amount of time it takes to

[32]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 1, 2005).

[33]GAO-10-142.

[34]GAO-08-683.

respond to an incident, and the percentage of BSAs completed on time. Some of these measures are also included in FPS's federal facilities security index, which is used to assess its performance. However, FPS has not developed outcome measures to evaluate the net effect of its efforts to protect GSA buildings. While output measures are helpful, outcome measures are also important because they can provide FPS with broader information on program results, such as the extent to which its decision to move to an inspector-based workforce will enhance security at GSA facilities or help identify the security gaps that remain at GSA facilities and determine what action may be needed to address them. In addition, FPS does not have a reliable data management system that will allow it to accurately track these measures or other important measures such as the number of crimes and other incidents occurring at GSA facilities. Without such a system, it is difficult for FPS to evaluate and improve the effectiveness of its efforts to protect federal employees and facilities, allocate its limited resources, or make informed risk management decisions. For example, weaknesses in one of FPS's countermeasure tracking systems make it difficult to accurately track the implementation status of recommended countermeasures such as security cameras and X-ray machines. Without this ability, FPS has difficulty determining whether it has mitigated the risk of GSA facilities to crime or a terrorist attack.

FPS Is Taking Steps to Better Protect GSA Buildings, but Has Not Fully Implemented Actions and Faces Significant Challenges

FPS is taking some steps in each of the key practice areas to improve its ability to better protect GSA buildings. Additionally, GAO has recommended that FPS implement specific actions to promote greater usage of key protection practices and otherwise improve security. However, FPS has not completed many related corrective actions and FPS faces implementation challenges as well.

FPS Is Developing a New Program to Assess Risk, Manage Human Capital, and Measure Performance

FPS is developing the Risk Assessment and Management Program (RAMP), which could enhance its approach to assessing risk, managing human capital, and measuring performance. With regard to improving the effectiveness of FPS's risk management approach and the quality of BSAs, FPS believes RAMP will provide inspectors with the information needed to make more informed and defensible recommendations for security countermeasures. FPS also anticipates that RAMP will allow inspectors to obtain information from one electronic source, generate reports

automatically, enable FPS to track selected countermeasures throughout their life cycle, address some concerns about the subjectivity inherent in BSAs, and reduce the amount of time inspectors and managers spend on administrative work. Additionally, FPS is designing RAMP so that it will produce risk assessments that are compliant with Interagency Security Committee standards, compatible with the risk management framework set forth by the National Infrastructure Protection Plan,[35] and consistent with the business processes outlined in the memorandum of agreement with GSA. According to FPS, RAMP will support all components of the BSA process, including gathering and reviewing building information; conducting and recording interviews; assessing threats, vulnerabilities, and consequences to develop a detailed risk profile; recommending appropriate countermeasures; and producing BSA reports. FPS also plans to use RAMP to track and analyze certain workforce data, contract guard program data, and other performance data such as the types and definitions of incidents and incident response times.

Although FPS intends for RAMP to improve its approach to risk assessment, human capital management, and performance measurement, it is not clear that FPS has fully addressed some implementation issues. For example, one issue concerns the accuracy and reliability of the information that will be entered into RAMP. According to FPS, the agency plans to transfer data from several of its legacy systems, including the Contract Guard Employment Requirements Tracking System (CERTS), into RAMP. In July 2009, we testified on the accuracy and reliability issues associated with CERTS.[36] FPS subsequently conducted an audit of CERTS to determine the status of its guard training and certification. However, the results of the audit showed that FPS was able to verify the status for about 7,600 of its 15,000 guards. According to an FPS official, one of its regions did not meet the deadline for submitting data to headquarters because its data were not accurate or reliable and therefore about 1,500 guards were not included in the audit. FPS was not able to explain why it was not able to verify the status of the remaining 5,900 guards. In 2008, we recommended that FPS develop and implement specific guidelines and standards for measuring its performance and improve how it categorizes,

[35]The National Infrastructure Protection Plan was in response to Homeland Security Presidential Directive 7 and sets forth national policy on how the plan's risk management framework and sector partnership model are to be implemented by sector-specific agencies. FPS is the agency responsible for the Government Facilities sector.

[36]GAO-09-859T.

collects, and analyzes data to help it better manage and understand the results of its efforts to protect GSA facilities and DHS concurred with our recommendations.[37] RAMP could be the vehicle through which FPS implements these recommendations, but the use of inaccurate and unreliable data will hamper performance measurement efforts.

Furthermore, it is unclear whether FPS will meet the implementation goals established in the program's proposed timeline. FPS began designing RAMP in early 2007 and expects to implement the program in three phases, completing its implementation by the end of fiscal year 2011. However, in June 2008, we reported that FPS was going to implement a pilot version of RAMP in fiscal year 2009,[38] but in May 2009, FPS officials told us they intend to implement the first phase in the beginning of fiscal year 2010. Until RAMP components are fully implemented, FPS will continue to rely on its current risk assessment tool, methodology, and process, potentially leaving GSA and tenant agencies dissatisfied. Additionally, FPS will continue to rely on its disparate workforce data management systems and CERTS or localized databases that have proven to be inaccurate and unreliable. We recently recommended that FPS provide the Secretary of Homeland Security with regular updates on the status of RAMP including the implementation status of deliverables, clear timelines for completion of tasks and milestones, and plans for addressing any implementation obstacles.[39] DHS concurred with our recommendation and stated that FPS will submit a monthly report to the Secretary.

FPS's Actions to Improve Guard Management May Be Difficult to Implement and Maintain

FPS took on a number of immediate actions with respect to contract guard management in response to our covert testing.

- For example, in July 2009, the Director of FPS instructed Regional Directors to accelerate the implementation of FPS's requirement that two guard posts at Level IV facilities be inspected weekly.
- FPS, in July 2009, also required more X-ray and magnetometer training for inspectors and guards. For example, FPS has recently issued an information bulletin to all inspectors and guards to provide them with

[37]GAO-08-863.

[38]GAO-08-683.

[39]GAO-10-142.

information about package screening, including examples of disguised items that may not be detected by magnetometers or X-ray equipment. Moreover, FPS produced a 15-minute training video designed to provide information on bomb component detection. According to FPS, each guard was required to read the information bulletin and watch the video within 30 days.

Despite the steps FPS has taken, there are a number of factors that will make implementing and sustaining these actions difficult. First, FPS does not have adequate controls to monitor and track whether its 11 regions are completing these new requirements. Thus, FPS cannot say with certainty that it is being done. According to a FPS regional official, implementing the new requirements may present a number of challenges, in part, because new directives appear to be based primarily on what works well from a headquarters or National Capital Region perspective, and not a regional perspective that reflects local conditions and limitations in staffing resources. In addition, another regional official estimated that his region is meeting about 10 percent of the required oversight hours and officials in another region said they are struggling to monitor the delivery of contractor-provided training in the region. Second, FPS has not completed any workforce analysis to determine if its current staff of about 930 law enforcement security officers will be able to effectively complete the additional inspections and provide the X-ray and magnetometer training to 15,000 guards, in addition to their current physical security and law enforcement responsibilities. According to the Director of FPS, while having more resources would help address the weaknesses in the guard program, the additional resources would have to be trained and thus could not be deployed immediately.

FPS Is Developing a Program to Standardize Equipment and Contracting

FPS is also taking steps to implement a more systematic approach to technology acquisition by developing a National Countermeasures Program, which could help FPS leverage technology more cost-effectively. According to FPS, the program will establish standards and national procurement contracts for security equipment, including X-ray machines, magnetometers, surveillance systems, and intrusion detection systems. FPS officials told us that instead of having inspectors search for vendors to establish equipment acquisition, installation, and maintenance contracts, inspectors will call an FPS mission support center with their countermeasure recommendations and the center will procure the services through standardized contracts. According to FPS, the program will also include life-cycle management plans for countermeasures. FPS

officials said they established an X-ray machine contract and that future program contracts will also explore the use of the schedule as a source for national purchase and service contracts. According to FPS, the National Countermeasures Program should provide the agency with a framework to better manage its security equipment inventory; meet its operational requirement to identify, implement, and maintain security equipment; and respond to stakeholders' needs by establishing nationwide resources, streamlining procurement procedures, and strengthening communications with its customers. FPS officials told us they believe this program will result in increased efficiencies because inspectors will not have to spend their time facilitating the establishment of contracts for security equipment because these contracts will be standardized nationwide.

Although the National Countermeasures Program includes improvements that may enhance FPS's ability to leverage technology, it does not establish tools for assessing the cost-effectiveness of competing technologies and countermeasures and implementation has been delayed. Security professionals are faced with a multitude of technology options offered by private vendors, including advanced intrusion detection systems, biotechnology options for screening people, and sophisticated video monitoring. Having tools and guidance to determine which technologies most cost-effectively address identified vulnerabilities is a central component of the leveraging technology key practice. FPS officials told us that the National Countermeasures Program will enable inspectors to develop countermeasure cost estimates that can be shared with GSA and tenant agencies. However, incorporating a tool for evaluating the cost-effectiveness of alternative technologies into FPS's planned improvements in the security acquisition area would represent an enhanced application of this key practice. Therefore, we recently recommended that FPS develop a methodology and guidance for assessing and comparing the cost-effectiveness of technology alternatives, and DHS concurred with our recommendation.[40]

Another concern is that FPS had planned to implement the program throughout fiscal year 2009, but extended implementation into fiscal year 2010, thus it is not clear whether FPS will meet the program's milestones in accordance with updated timelines. Until the National Countermeasures Program is fully implemented, FPS will continue to rely on individual inspectors to make technology decisions. For example, FPS had

[40]GAO-10-142.

anticipated that the X-ray machine and magnetometer contracts would be awarded by December 2008, and that contracts for surveillance and intrusion detection systems would be awarded during fiscal year 2009. In May 2009, FPS officials told us that the X-ray machine contract was awarded on April 30, 2009, and that they anticipated awarding the magnetometer contract in the fourth quarter of fiscal year 2009 and an electronic security services contract for surveillance and intrusion detection systems during the second quarter of fiscal year 2010. We recently recommended that FPS provide the Secretary of Homeland Security with regular updates on the status of the National Countermeasures Program, including the implementation status of deliverables, clear timelines for completion of tasks and milestones, and plans for addressing any implementation obstacles.[41] DHS concurred with this recommendation and stated that FPS will submit a monthly report to the Secretary.

Key Practices Provide a Framework for Improvement for FPS and Other Agencies

Finally, as we stated at the outset, the protection of federal real property has been and continues to be a major concern. Therefore, we have used our key protection practices as criteria to evaluate the security efforts of other departments, agencies, and entities and have made recommendations to promote greater usage of key practices in ensuring the security of public spaces and of those who work at and visit them. For example, we have examined how DHS[42] and the Smithsonian Institution[43] secure their assets and identified challenges. Most recently, we evaluated the National Park Service's (Park Service) approach to national icon and park protection.[44] We found that although the Park Service has implemented a range of security program improvements in recent years that reflected some aspects of key practices, there were also limitations. Specifically, the Park Service (1) does not manage risk servicewide or

[41]GAO-10-142.

[42]GAO, *Federal Real Property: DHS Has Made Progress, but Additional Actions Are Needed to Address Real Property Management and Security Challenges*, GAO-07-658 (Washington, D.C.: June 22, 2007). In this report, we used the key practices to assess DHS's security operations with respect to the government-owned and leased buildings in its real property portfolio, but did not specifically focus on FPS.

[43]GAO, *Smithsonian Institution: Funding Challenges Affect Facilities' Conditions and Security, Endangering Collections*, GAO-07-1127 (Washington, D.C.: Sept. 28, 2007).

[44]GAO, *Homeland Security: Actions Needed to Improve Security Practices at National Icons and Parks*, GAO-09-983 (Washington, D.C.: Aug. 28, 2009).

ensure the best return on security technology investments; (2) lacks a servicewide approach to sharing information internally and measuring performance; and (3) lacks clearly defined security roles and a security training curriculum. With millions of people visiting the nation's nearly 400 park units annually, ensuring their security and the protection of our national treasures is paramount. More emphasis on the key practices would provide greater assurance that Park Service assets are well protected and that Park Service resources are being used efficiently to improve protection.

FPS faces challenges that are similar, in many respects, to those that agencies across the government are facing. Our key practices provide a framework for assessing and improving protection practices, and in fact, the Interagency Security Committee is using our key facility protection practices as key management practices to guide its priorities and work activities. For example, the committee established subcommittees for technology best practices and training, and working groups in the areas of performance measures and strategic human capital management. The committee also issued performance measurement guidance in 2009.[45] Without greater attention to key protection practices, FPS will be ill equipped to efficiently and effectively fulfill its responsibilities of assessing risk, strategically managing its workforce and contract guard program, recommending countermeasures, sharing information and coordinating with GSA and tenant agencies to secure GSA buildings, and measuring and testing its performance as the security landscape changes and new threats emerge. Furthermore, implementing our specific recommendations related to areas such as human capital and risk management will be critical steps in the right direction. Overall, following this framework—adhering to key practices and implementing recommendations in specific areas—would enhance FPS's chances for future success and could position FPS to become a leader and benchmark agency for facility protection in the federal government.

Mr. Chairman, this concludes our testimony. We are pleased to answer any questions you might have.

[45]Interagency Security Committee, *Use of Physical Security Performance Measures*, (Washington, D.C., June 16, 2009).

Contact Information

For further information on this testimony, please contact Mark L. Goldstein at (202) 512-2834 or by e-mail goldsteinm@gao.gov. Individuals making key contributions to this testimony include Tammy Conquest, John Cooney, Elizabeth Eisenstadt, Brandon Haller, Denise McCabe, David Sausville, and Susan Michal-Smith.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548