

GAO

Testimony

Before the Subcommittee on Economic  
Development, Public Buildings and  
Emergency Management, Committee on  
Transportation and Infrastructure

---

For Release on Delivery  
Expected at 2:00 p.m. EDT  
Wednesday, September 23, 2009

**HOMELAND SECURITY**

**Federal Protective Service  
Has Taken Some Initial  
Steps to Address Its  
Challenges, but  
Vulnerabilities Still Exist**

Statement of Mark L. Goldstein, Director  
Physical Infrastructure Team



**GAO**

Accountability \* Integrity \* Reliability

---



Highlights of [GAO-09-1047T](#), a testimony to Subcommittee on Economic Development, Public Buildings and Emergency Management, House Committee on Transportation and Infrastructure

## Why GAO Did This Study

To accomplish its mission of protecting federal facilities, the Federal Protective Services (FPS), within the Department of Homeland Security (DHS), currently has a budget of about \$1 billion, about 1,200 full-time employees, and about 15,000 contract security guards.

This testimony is based on completed and ongoing work for this Subcommittee and discusses: (1) challenges FPS faces in protecting federal facilities and (2) how FPS's actions address these challenges. To perform this work, GAO visited FPS's 11 regions, analyzed FPS data, and interviewed FPS officials, guards, and contractors. GAO also conducted covert testing at 10 judgmentally selected level IV facilities in four cities. Because of the sensitivity of some of the information, GAO cannot identify the specific locations of incidents discussed. A level IV facility has over 450 employees and a high volume of public contact.

## What GAO Recommends

GAO has ongoing work on FPS and plans to report its complete evaluation along with any recommendations at a later date.

View [GAO-09-1047T](#) or [key components](#). For more information, contact Mark Goldstein at (202) 512-2834 or [goldsteinm@gao.gov](mailto:goldsteinm@gao.gov).

## HOMELAND SECURITY

### Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist

#### What GAO Found

FPS faces challenges that hamper its ability to protect government employees and members of the public who work in and visit federal facilities. First, as we reported in our June 2008 report, FPS does not have a risk management framework that links threats and vulnerabilities to resource requirements. Without such a framework, FPS has little assurance that its programs will be prioritized and resources will be allocated to address changing conditions. Second, as discussed in our July 2009 report, FPS lacks a strategic human capital plan to guide its current and future workforce planning efforts. FPS does not collect data on its workforce's knowledge, skills, and abilities and therefore cannot determine its optimal staffing levels or identify gaps in its workforce and determine how to fill these gaps. Third, as we testified at a July 2009 congressional hearing, FPS's ability to protect federal facilities is hampered by weaknesses in its contract security guard program. GAO found that many FPS guards do not have the training and certifications required to stand post at federal facilities in some regions. For example, in one region, FPS has not provided the required 8 hours of X-ray or magnetometer training to its 1,500 guards since 2004. GAO also found that FPS does not have a fully reliable system for monitoring and verifying whether guards have the training and certifications required to stand post at federal facilities. In addition, FPS has limited assurance that guards perform assigned responsibilities (post orders). Because guards were not properly trained and did not comply with post orders, GAO investigators with the components for an improvised explosive device concealed on their persons, passed undetected through access points controlled by FPS guards at 10 of 10 level IV facilities in four major cities where GAO conducted covert tests.

FPS has taken some actions to better protect federal facilities, but it is difficult to determine the extent to which these actions address these challenges because many of the actions are recent and have not been fully implemented. Furthermore, FPS has not fully implemented several recommendations that GAO has made over the last couple of years to address FPS's operational and funding challenges, despite the Department of Homeland Security's concurrence with the recommendations. In addition, most of FPS's actions focus on improving oversight of the contract guard program and do not address the need to develop a risk management framework or a human capital plan. To enhance oversight of its contract guard program FPS is requiring its regions to conduct more guard inspections at level IV facilities and provide more x-ray and magnetometer training to inspectors and guards. However, several factors make these actions difficult to implement and sustain. For example, FPS does not have a reliable system to track whether its 11 regions are completing these new requirements. Thus, FPS cannot say with certainty that the requirements are being implemented. FPS is also developing a new information system to help it better protect federal facilities. However, FPS plans to transfer data from several of its legacy systems, which GAO found were not fully reliable or accurate, into the new system.

---

Madam Chair and Members of the Subcommittee:

We are pleased to be here to discuss the Federal Protective Service's (FPS) efforts to ensure the protection of the over 1 million government employees, as well as members of the public, who work in and visit the nation's 9,000 federal facilities each year.<sup>1</sup> 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, Oklahoma. Nevertheless, the recent shooting death of a guard at the U.S. Holocaust Memorial Museum—though not a federal facility—demonstrates the continued vulnerability of public buildings to domestic terrorist attack. To accomplish its mission of protecting federal facilities, FPS currently has a budget<sup>2</sup> of about \$1 billion, about 1,200 full time employees, and about 15,000 contract security guards deployed at federal facilities across the country.

As the primary federal agency that is responsible for protecting and securing General Services Administration (GSA) facilities and federal employees and visitors across the country, FPS has the authority to enforce federal laws and regulations aimed at protecting federally owned and leased properties and the persons on such property. FPS conducts its mission by providing security services through two types of activities: (1) physical security activities—conducting threat assessments of facilities and recommending risk-based 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.

---

<sup>1</sup>For the purposes of this report, federal facilities are the 9,000 buildings under the control or custody of General Services Administration (GSA).

<sup>2</sup>Funding for FPS is provided through revenues and collections 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 operations.

---

This testimony is based on completed<sup>3</sup> and ongoing work<sup>4</sup> for this Subcommittee and discusses (1) challenges FPS faces in protecting federal facilities and (2) how FPS's actions address these challenges. To perform this work, we visited FPS's 11 regions, analyzed FPS data, and interviewed FPS officials, guards, and contractors. We also conducted covert testing at 10 judgmentally selected high risk facilities in four cities. Because of the sensitivity of some of the information in our report, we cannot specifically identify the locations of the incidents discussed. We conducted this performance audit from April 2007 to September 2009 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.

---

## FPS Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities

FPS faces a number of challenges that hamper its ability to protect government employees and the public in federal facilities. For example, these challenges include (1) developing a risk management framework, (2) developing a human capital plan, and (3) better oversight of its contract security guard program.

---

## FPS Has Not Implemented a Risk Management Framework for Identifying Security Requirements and Allocating Resources

In our June 2008 report we found that in protecting federal facilities, FPS does not use a risk management approach that links threats and vulnerabilities to resource requirements. We have stated that without a risk management approach that identifies threats and vulnerabilities and the resources required to achieve FPS's security goals, there is little assurance that programs will be prioritized and resources will be allocated

---

<sup>3</sup>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), 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), and 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).

<sup>4</sup>We plan to provide Congress with our complete evaluation at a later date.

---

to address existing and potential security threats in an efficient and effective manner. While FPS has conducted risk related activities such as building security assessments (BSAs), we have reported several concerns with the Facilities Securities Risk Management system FPS currently uses to conduct these assessments. First, it does not allow FPS to compare risks from building to building so that security improvements to buildings can be prioritized across GSA's portfolio. Second, current risk assessments need to be categorized more precisely. According to FPS, too many BSAs are categorized as high or low risk, which does not allow for a refined prioritization of security improvements. Third, the system does not allow for tracking the implementation status of security recommendations based on assessments.

BSAs are the core component of FPS's physical security mission. However, ensuring the quality and timeliness of them is an area in which FPS continues to face challenges. Many law enforcement security officers (LESOs)<sup>5</sup> in the regions we visited stated that they do not have enough time to complete BSAs. For example, while FPS officials have stated that BSAs for level IV facilities<sup>6</sup> should take between 2 to 4 weeks, several LESOs reported having only 1 or 2 days to complete assessments for their buildings, in part, because of pressure from supervisors to complete BSAs as quickly as possible. Some regional supervisors have also found problems with the accuracy of BSAs. One regional supervisor reported that an inspector was repeatedly counseled and required to redo BSAs when supervisors found he was copying and pasting from previous assessments. Similarly, one regional supervisor stated that in the course of reviewing a BSA for an address he had personally visited, he realized that the inspector completing the BSA had not actually visited the site because

---

<sup>5</sup>LESOs who are also referred to as inspectors are responsible for completing building security assessments and oversight of contract guards.

<sup>6</sup>The level of security FPS provides at each of the 9,000 federal facilities varies depending on the building's security level. Based on the Department of Justice's (DOJ) 1995 Vulnerability Assessment Guidelines, there are five types of security levels. A level I facility is typically a small storefront -type operation such as military recruiting office which has 10 or fewer employees and a low volume of public contact. A level II facility has from 11 to 150 employees, a level III facility has from 151 to 450 federal employees and moderate to high volume of public contact, a level IV facility has over 450 employees, a high volume of public contact, and includes high risk law enforcement and intelligence agencies. FPS does not have responsibility for a Level V facility which include the White House and the Central Intelligence Agency. The Interagency Security Committee has recently promulgated new security level standards that will supersede the 1995 DOJ standards.

---

the inspector referred to a large building when the actual site was a vacant plot of land owned by GSA.

Moreover, some GSA and FPS officials have stated that LESOs lack the training and physical security expertise to prepare BSAs according to the standards. Currently, LESOs receive instructions on how to complete BSAs as part of a 4-week course at the Federal Law Enforcement Training Center's Physical Security Training Program. However, many LESOs and supervisors in the regions we visited stated that this training is insufficient and that refresher training is necessary to keep LESOs informed about emerging technology, but that this refresher training has not been provided in recent years. Regional GSA officials also stated that they believe the physical security training provided to LESOs is inadequate and that it has affected the quality of the BSAs they receive.

Further complicating FPS's ability to protect federal facilities is the building security committee structure. Building Security Committees (BSC) are composed of representatives from each tenant agency who generally are not security professionals but have responsibility for approving the countermeasures FPS recommends. However, in some of the facilities that we visited, security countermeasures were not implemented because BSC members could not agree on what countermeasures to implement or were unable to obtain funding from their agencies. For example, an FPS official in a major metropolitan city stated that over the last 4 years LESOs have recommended 24-hour contract guard coverage at one high-risk building located in a high crime area multiple times, but the BSC is not able to obtain approval from all its members.

In addition, 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.<sup>7</sup> FPS charges federal agencies the same basic security fee regardless of the perceived threat to a particular

---

<sup>7</sup>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.

---

building or agency. In fiscal year 2009, FPS is charging 66 cents per square foot for basic security. Although FPS categorizes buildings according to security levels<sup>8</sup> based on its assessment of each building's risk and size, this assessment does not 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 small post office or 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.

FPS's basic security rate has raised questions about equity because federal agencies are required to pay the fee regardless of the level of service FPS provides or the cost of providing the service. For instance, in some of the regions we visited, FPS officials described situations where staff are stationed hundreds of miles from buildings under its responsibility, with many of these buildings rarely receiving services from FPS staff and relying mostly on local law enforcement agencies for law enforcement services. However, FPS charges these tenant agencies the same basic security fees as buildings in major metropolitan areas where numerous FPS police officers and LESOs are stationed and are available to provide security services. Consequently, FPS's cost of providing services is not reflected in its basic security charges. 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 July 2008 report, we recommended that FPS improve FPS's 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. While DHS agreed with this recommendation, FPS has not fully implemented it.

---

<sup>8</sup>These levels range from I (lowest risk) to IV (highest risk).

---

## FPS Does Not Have A Strategic Human Capital Plan to Guide Its Current and Future Workforce Planning Efforts

In our July 2009 report,<sup>9</sup> we reported that FPS does not have a strategic human capital plan to guide its current and future workforce planning efforts. Our work has shown that a strategic human capital plan addresses two critical needs: It (1) aligns an organization's human capital program with its current and emerging mission and programmatic goals, and (2) develops long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals. In 2007, FPS took steps toward developing a Workforce Transition Plan to reflect its decision to move to a LESO-based workforce and reduce its workforce to about 950 employees. However, in 2008, FPS discontinued this plan because the objective of the plan—to reduce FPS staff to 950 to meet the President's Fiscal Year 2008 Budget—was no longer relevant because of the congressional mandate in its Fiscal Year 2008 Consolidated Appropriations Act to increase its workforce to 1,200 employees.<sup>10</sup> FPS subsequently identified steps it needed to take in response to the mandate. However, we found that these steps do not include developing strategies for determining agency staffing needs, identifying gaps in workforce critical skills and competencies, developing strategies for use of human capital flexibilities, or strategies for retention and succession planning.

Moreover, we found FPS's headquarters does not collect data on its workforce's knowledge, skills, and abilities. Consequently, FPS cannot determine what its optimal staffing levels should be or identify gaps in its workforce needs and determine how to modify its workforce planning strategies to fill these gaps. Effective workforce planning requires consistent agencywide data on the skills needed to achieve current and future programmatic goals and objectives. Without centralized or standardized data on its workforce, it is unclear how FPS can engage in short- and long-term strategic workforce planning. Finally, FPS's human capital challenges may be further exacerbated by a proposal in the President's 2010 budget to move FPS from Immigration and Custom Enforcement to the National Protection and Programs Directorate within DHS. If the move is approved, it is unclear which agency will perform the human capital function for FPS, or how the move will affect FPS's operational and workforce needs. We also recommended that FPS take steps to develop a strategic human capital plan to manage its current and future workforce needs. FPS concurred with our recommendation.

---

<sup>9</sup>GAO-09-749.

<sup>10</sup>Pub. L. No. 110-161, Division E, 121 Stat. 1844, 2051-2052 (2007).

---

## FPS's Ability to Protect Federal Facilities Is Hampered by Weaknesses in Its Contract Guard Program

FPS's contract guards are the most visible component of FPS's operations as well as the public's first contact with FPS when entering a federal facility. Moreover, FPS relies heavily on its guards and considers them to be the agency's "eyes and ears" while performing their duties. However, as we testified at a July 2009 congressional hearing, FPS does not fully ensure that its guards have the training and certifications required to be deployed to a federal facility. While FPS requires that all prospective guards complete approximately 128 hours of training, including 8 hours of x-ray and magnetometer training, FPS was not providing some of its guards with all of the required training in the six regions we visited. For example, in one region, FPS has not provided the required 8 hours of x-ray or magnetometer training to its 1,500 guards since 2004. X-ray and magnetometer training is important because the majority of the guards are primarily responsible for using this equipment to monitor and control access points at federal facilities. According to FPS officials, the 1,500 guards were not provided the required x-ray or magnetometer training because the region does not have employees who are qualified or have the time to conduct the training. Nonetheless, these guards continue to control access points at federal facilities in this region. In absence of the x-ray and magnetometer training, one contractor in the region said that they are relying on veteran guards who have experience operating these machines to provide some "on-the-job" training to new guards. Moreover, in the other five regions we visited where FPS is providing the x-ray and magnetometer training, some guards told us that they believe the training, which is computer based, is insufficient because it is not conducted on the actual equipment located at the federal facility.

Lapses and weaknesses in FPS's x-ray and magnetometer training have contributed to several incidents at federal facilities in which the guards were negligent in carrying out their responsibilities. For example, at a level IV federal facility in a major metropolitan area, an infant in a carrier was sent through the x-ray machine. 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.<sup>11</sup> Because the guard was not paying attention and the machine's safety features had been disabled,<sup>12</sup> the infant in the carrier was sent through the x-ray machine. x-

---

<sup>11</sup>X-ray machines are hazardous because of the potential radiation exposure. In contrast, magnetometers do not emit radiation and are used to detect metal.

<sup>12</sup>With this safety feature disabled, the x-ray machine's belt was operating continuously although the guard was not present.

---

ray machines are hazardous because of the potential radiation exposure. 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.

Moreover, FPS's primary system—Contract Guard Employment Requirements Tracking System (CERTS)—for monitoring and verifying whether guards have the training and certifications required to stand post at federal facilities is not fully reliable. We reviewed training and certification data for 663 randomly selected guards in 6 of FPS's 11 regions maintained either in CERTS, which is the agency's primary system for tracking guard training and certifications, databases maintained by some regions, or contractor information. We found that 62 percent, or 411 of the 663 guards who were deployed to a federal facility had at least one expired certification, including for example, firearms qualification, background investigation, domestic violence declaration, or CPR/First Aid training certification. Without domestic violence declarations certificates, guards are not permitted to carry a firearm. In addition, not having a fully reliable system to better track whether training has occurred may have contributed to a situation in which a contractor allegedly falsified training records. In 2007, FPS was not aware that a contractor who was responsible for providing guard service at several level IV facilities in a major metropolitan area had allegedly falsified training records until it was notified by an employee of the company. According to FPS's affidavit, the contractor allegedly repeatedly self-certified to FPS that its guards had satisfied CPR and First Aid training, as well as the contractually required bi-annual recertification training, although the contractor knew that the guards had not completed the required training and was not qualified to stand post at federal facilities. According to FPS's affidavit, in exchange for a \$100 bribe, contractor officials provided a security guard with certificates of completion for CPR and First Aid. The case is currently being litigated in U.S. District Court.

FPS has limited assurance that its 15,000 guards are complying with post orders once they are deployed to federal facilities. At each guard post, FPS maintains a book, referred to as post orders, that describes the duties that guards are to perform while on duty. According to post orders, guards have many duties, including access and egress control, operation of security equipment, such as x-ray and magnetometer, detecting, observing and reporting violations of post regulations, and answering general

---

questions and providing directions to visitors and building tenants, among others. We found that in the 6 regions we visited that guard inspections are typically completed by FPS during regular business hours and in cities where FPS has a field office. In most FPS regions, FPS is only on duty during regular business hours and according to FPS, LESOs are not authorized overtime to perform guard inspections during night shifts or on weekends. However, on the few occasions when LESOs complete guard inspections at night or on their own time, FPS has found instances of guards not complying with post orders. For example, at a level IV facility, an armed guard was found asleep at his post after taking the pain killer prescription drug Percocet during the night shift. FPS's guard manual states that guards are not permitted to sleep or use any drugs (prescription or non-prescription) that may impair the guard's ability to perform duties.

Finally, we identified substantial security vulnerabilities related to FPS's guard program. Each time they tried, our investigators successfully passed undetected through security checkpoints monitored by FPS guards, with the components for an IED concealed on their persons at 10 level IV facilities in four cities in major metropolitan areas. 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 we penetrated, 8 were government owned and 2 were leased facilities. The facilities included field offices of a U.S Senator and 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 point 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.<sup>13</sup> To gain entry into each of the 10 level IV facilities, our investigators showed photo identification (state driver's license) and walked through the magnetometer machines without incident. The 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 we 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 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.

Despite increased awareness of security vulnerabilities at federal facilities, recent FPS penetration testing—similar to the covert testing we conducted in May 2009—showed that weaknesses in FPS's contract guard training continue to exist. In August 2009, we accompanied FPS on a test of security countermeasures at a level IV facility. During these tests, FPS agents placed a bag on the x-ray machine belt containing a fake gun and knife. The guard failed to identify the gun and knife on the x-ray screen and the undercover FPS official was able to retrieve his bag and proceed to the check-in desk without incident. During a second test, a knife was hidden on a FPS officer. During the test, the magnetometer detected the knife, as did the hand wand, but the guard failed to locate the knife and the FPS officer was able to gain access to the facility. According to the FPS officer, the guards who failed the test had not been provided the required x-ray and magnetometer training. Upon further investigation, only two of the eleven guards at the facility had the required x-ray and magnetometer training. However, FPS personnel in its mobile command vehicle stated

---

<sup>13</sup>Tests that we performed at a national laboratory in July 2007 and in February 2006, 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.

---

that the 11 guards had all the proper certifications and training to stand post. It was unclear at the time, and in the after action report, whether untrained guards were allowed to continue operating the x-ray and magnetometer machines at the facilities or if FPS's LESOs stood post until properly trained guards arrived on site.

---

## FPS Has Recently Taken Some Actions to Better Protect Federal Facilities, However Many are Not Fully Implemented

While FPS has taken some actions to improve its ability to better protect federal facilities, it is difficult to determine the extent to which these actions address these challenges because most of them occurred recently and have not been fully implemented. It is also important to note that most of the actions FPS has recently taken focus on improving oversight of the contract guard program and do not address the need to develop a risk management framework and a human capital plan. In response to our covert testing, FPS has taken a number of actions. 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 also required more x-ray and magnetometer training for LESOs and guards. For example, FPS has recently issued an information bulletin to all LESOs and guards to provide them with 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 DVD within 30 days.

However, 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 directive appears 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, according to FPS

---

officials, it has not modified any of its 129 guard contracts to reflect these new requirements, and therefore the contractors are not obligated to implement these requirements. One contractor stated that ensuring that its guards receive the additional training will be logistically challenging. For example, to avoid removing a guard from his/her post, one contractor plans to provide some of the training during the guards' 15 minute breaks. Third, 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. Our previous work has raised questions about the wide range of responsibilities LESOs have and the quality of BSAs and guard oversight. 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.

In addition, as we reported in June 2008, FPS is in the process of developing a new system referred to as the Risk Assessment Management Program (RAMP). According to FPS, RAMP will be the primary tool FPS staff will use to fulfill their mission and is designed to be a comprehensive, systematic, and dynamic means of capturing, accessing, storing, managing, and utilizing pertinent facility information. RAMP will replace several legacy GSA systems that FPS brought to DHS, including CERTS, Security Tracking System, and other systems associated with the BSA program. We are encouraged that FPS is attempting to replace some of its legacy GSA systems with a more reliable and accurate system. However, we are not sure FPS has fully addressed some issues associated with implementing RAMP. For example, we are concerned about 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 CERTS into RAMP. In July 2009, we reported on the accuracy and reliability issues associated with CERTS. 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 was 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. FPS expects RAMP to be fully operational in 2011, however until that time FPS will continue to rely on its current CERTS system or localized databases that have proven to be inaccurate and unreliable.

---

Finally, over the last couple of years we have completed a significant amount of work related to challenges described above and made recommendations to address these challenges. While DHS concurred with our recommendations, FPS has not fully implemented them. In addition, in October 2009, we plan to issue a public report on FPS key practices involving risk management, leveraging technology and information sharing and coordination.

---

This concludes our testimony. We are pleased to answer any questions you might have.

---

## Contact Information

For further information on this testimony, please contact Mark Goldstein at 202-512-2834 or by email [goldsteinm@gao.gov](mailto:goldsteinm@gao.gov). Individuals making key contributions to this testimony include Tida Barakat, Jonathan Carver, Tammy Conquest, Bess Eisenstadt, Daniel Hoy, Susan Michal-Smith, and Lacy Vong.

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

---

## 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](http://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](http://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](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto: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](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

