United States Government Accountability Office

GAO

Report to the Chairman, Committee on Homeland Security, House of Representatives

October 2009

HOMELAND SECURITY

Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection

GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-142, a report to the Chairman, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

There is ongoing concern about the security of federal buildings and their occupants. 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 buildings 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 that included: *allocating resources using risk management*, *leveraging technology*, and *information sharing and coordination*. As requested, GAO determined whether FPS's security efforts for GSA buildings reflected key practices. To meet this objective, GAO used its key practices as criteria, visited five sites to gain firsthand knowledge, analyzed pertinent DHS and GSA documents, and interviewed DHS, GSA, and tenant agency officials.

What GAO Recommends

GAO is making three recommendations to the Secretary of Homeland Security. These include instructing FPS to report regularly to the Secretary on its new risk management and countermeasures programs, develop guidance for cost-effectively leveraging technology, and determine information sharing parameters with GSA. DHS concurred with the report's recommendations.

View GAO-10-142 or key components.
For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

October 2009

HOMELAND SECURITY

Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection

What GAO Found

FPS's approach to securing GSA buildings reflects some aspects of key protection practices, and FPS has several improvements underway such as a new risk assessment program and a countermeasure acquisition program. While FPS's protection activities exhibit some aspects of the key practices, GAO found limitations in each of the areas.

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 FPS's countermeasure recommendations. Moreover, FPS uses an outdated risk assessment tool and a subjective, time-consuming process. As a result, GSA and tenant agencies are uncertain whether risks are being mitigated. Concerned with the quality and timeliness of FPS's risk assessment services, GSA and tenant agencies are pursuing some of these activities on their own. Although FPS is developing a new risk management program, full implementation is not planned until the end of fiscal year 2011 and has already experienced delays.

With regard to *leveraging technology*, FPS inspectors have considerable latitude for selecting technologies and countermeasures that tenant agencies fund, but FPS provides inspectors with little training and guidance for making cost-effective choices. Additionally, FPS does not provide tenant agencies with an analysis of alternative technologies, their cost, and 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. Although FPS is developing a program to standardize security equipment and contracting, the program has run behind schedule and lacks an evaluative component for assessing the cost-effectiveness of competing technologies and countermeasures.

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. Lack of coordination through regular contact can lead to communication breakdowns. For example, during a construction project at one location, the surveillance equipment that FPS was responsible for maintaining was removed from the site during 2007. FPS and tenant agency representatives disagree over whether FPS was notified of this action. Furthermore, FPS and GSA disagree over what building risk assessment information can be shared. FPS maintains that the sensitive information contained in the assessments is not needed for GSA to carry out its mission. However, GSA maintains that restricted access to the risk assessments constrains its ability to protect buildings and occupants.

Contents

Abbreviations

BSA	building security assessment
BSC	building security committee
DHS	Department of Homeland Security
DOJ	Department of Justice
FAS	Federal Acquisition Service
FPS	Federal Protective Service
GSA	General Services Administration
HSPD-7	Homeland Security Presidential Directive 7
HSPD-12	Homeland Security Presidential Directive 12
ICE	U.S. Immigration and Customs Enforcement
ISC	Interagency Security Committee
LES	Law Enforcement Sensitive
MOA	memorandum of agreement
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
PBS	Public Buildings Service
RAMPART	Risk Assessment Methodology Property Analysis and Ranking Tool
RAMP	Risk Assessment and Management Program
SBU	Sensitive But Unclassified
SWA	Security Work Authorization

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 23, 2009

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

Concerns persist about the security of federal buildings, their occupants, and visitors to these buildings. The Federal Protective Service (FPS) provides law enforcement and related security services for the nearly 9,000 buildings that are under the control and custody of the General Services Administration (GSA). FPS's services include—but are not limited to—responding to incidents and demonstrations, conducting risk assessments, participating in meetings with GSA property managers and tenant agencies, and determining whether GSA buildings are compliant with security standards established by the Interagency Security Committee (ISC).[1] GSA serves as the federal government's landlord and designs, builds, and manages facilities to support the needs of other federal agencies. Until 2003, FPS was a component of GSA's Public Buildings Service (PBS), but the Homeland Security Act of 2002 transferred FPS to the Department of Homeland Security (DHS)[2] and DHS placed FPS within U.S. Immigration and Customs Enforcement (ICE). Under the act, FPS retained its law enforcement and related security functions for GSA buildings and grounds, while GSA retained its powers, functions, and authorities related to the operation, maintenance, and protection of GSA buildings and grounds.[3] To guide the transition, DHS and GSA developed a Memorandum of Agreement (MOA) to set forth roles, responsibilities, and operational relationships between FPS and GSA concerning the protection of GSA buildings. Additionally, in 2006, GSA established a security division

[1] 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. ISC has representation from all major federal departments and agencies. In 2003, the Chair of the ISC moved from GSA to DHS.

[2] 6 U.S.C. § 203.

[3] 6 U.S.C. § 232.

within PBS to oversee its security operations and policies and liaise with FPS. The President's Budget for Fiscal Year 2010 proposed transferring FPS from ICE to the National Protection and Programs Directorate (NPPD) within DHS.[4]

We have identified a set of key facility protection practices from the collective practices of federal agencies and the private sector to provide a framework for guiding agencies' protection efforts and addressing challenges.[5] In this report, we use these key practices to evaluate how FPS protects GSA buildings. The key practices essentially form the foundation of a comprehensive approach to building protection.[6] ISC is using our key facility protection practices to guide its priorities and work activities. We focused on the following three key practices for this report:[7]

- *Allocating 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.

- *Leveraging technology.* Select technologies to enhance asset security through methods like access control, detection, and surveillance systems. This involves not only using technology, but ensuring that

[4] According to the DHS budget for fiscal year 2010, FPS is to be transferred from ICE to NPPD because FPS's responsibilities are outside the scope of ICE's immigration and customs enforcement mission and are better aligned to NPPD.

[5] 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).

[6] We have used these key practices as criteria to evaluate how entities such as DHS and the Smithsonian Institution secure their assets. 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). GAO, *Smithsonian Institution: Funding Challenges Affect Facilities' Conditions and Security, Endangering Collections*, GAO-07-1127 (Washington, D.C.: Sept. 28, 2007).

[7] For the purposes of this review, we did not include key practices related to (1) performance measurement and testing, because we reported on the limitations FPS faces in assessing its performance 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); (2) aligning assets to mission because GSA, not FPS, controls the asset inventory; and (3) strategic management of human capital because we are reviewing FPS's management of human capital in a separate engagement. Appendix I explains our methodology in detail.

there are positive returns on investment 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.

You requested that we determine whether FPS's approach to securing GSA buildings reflects key facility protection practices. In response, on July 29, 2009, we issued a sensitive but unclassified report. As that report contained information that was deemed to be either law enforcement sensitive or for official use only, this version of the report is intended to communicate our findings and recommendations as related to each of the key practices that we reviewed while omitting sensitive information about building security, including specific vulnerabilities.

To meet the objective, we used the three key practices cited above as a framework for assessing facility protection efforts by FPS management and at the individual buildings. In doing our work, we reviewed pertinent documents and policies from FPS and GSA, related laws and directives, ISC's security standards, and prior and ongoing GAO work. We also interviewed FPS and GSA officials at the national and regional levels, and the ISC executive director. We selected five sites to illustrate how FPS protects highly visible GSA buildings, basing our selection on factors that included geographical diversity, occupancy, the building's security level,[8] and other potential security considerations, such as new or planned construction. Selected sites included three multitenant level IV buildings,[9]

[8] At the time of our review, FPS evaluated the security level of GSA's facilities using Department of Justice (DOJ) standards that categorized facilities from level I (low risk) to level V (high risk).

[9] 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.

one single-tenant level IV campus,[10] and one single-tenant level III campus.[11]

At these sites, we collected documentation and interviewed officials from FPS, GSA, and tenant agencies. To supplement these site visits, we interviewed FPS and GSA security officials from the four regions where we had visited buildings. Because we observed FPS's efforts to protect GSA buildings at a limited number of sites, our observations of security issues at specific buildings cannot be generalized to all the buildings that FPS is responsible for securing. We conducted this performance audit from January 2008 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. Appendix I contains a more detailed discussion of our scope and methodology.

Results in Brief

FPS's approach to securing GSA buildings reflects some aspects of the key facility protection practices we examined—*allocating resources using risk management, leveraging technology, and information sharing and coordination*—but we also found significant limitations. FPS recognizes the importance of making progress in these areas and has improvements underway that could bring its activities more in line with the key practices and better equip FPS to address security vulnerabilities at GSA-controlled federal buildings. For example, FPS is developing a new risk assessment tool and standardizing technology acquisition. However, until these measures are fully implemented, FPS will continue to rely on its current methods, which fall short of a comprehensive approach to facility protection rooted in key practices. More specifically:

- FPS assesses risk and recommends countermeasures to GSA and tenant agencies; however, FPS's ability to influence the *allocation of*

[10] According to ISC facility security level determinations standards, a campus consists of two or more federal facilities located contiguous to one another and typically sharing some aspects of the environment—such as parking, courtyards, private vehicle access roads or gates, or entrances to connected facilities.

[11] 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.

resources using risk management is limited because resource allocation decisions are the responsibility of GSA and tenant agencies, which may be unwilling to fund FPS's countermeasure recommendations. We have found that under this 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. For example, one location shared a surveillance system with an adjacent federal location, and while one building security committee (BSC) agreed to fund a surveillance system upgrade that FPS had recommended, the BSC of the other location would not, thus adversely affecting the security of both locations. 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 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. FPS is developing a new risk management program that is intended to incorporate a new risk assessment tool and be less subjective and time-consuming. However, according to FPS's plans, this program will not be fully implemented until the end of fiscal year 2011, and its development has already been delayed.

- *Leveraging technology* is a key practice over which FPS has somewhat more control. 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. 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. At one location, for example, FPS recommended that in addition to using an explosives detection dog to screen mail, an enhanced X-ray machine should be used to detect additional hazardous agents to lower the threat level. However, FPS did not include a cost analysis of the countermeasure and risk options in the BSA executive summary, leaving tenant agency representatives without key information for making a decision with cost and risk implications. FPS is developing a program to standardize its security equipment recommendations and contracting, but until the program is fully implemented, individual inspectors will continue to make recommendations based on individual judgment and information from vendors. In addition, FPS had planned to implement the new program during fiscal year 2009, but extended full implementation into fiscal year 2010. Moreover, the program does not provide for assessing the cost-effectiveness of competing technologies and countermeasures.

- *Information sharing and coordination* occur in a variety of ways, and FPS and GSA top management have established communication channels. However, the types of information shared at the regional and building levels are inconsistent, and FPS and GSA disagree over what information should be shared. For example, the MOA between DHS and GSA specifies that FPS will provide quarterly briefings at the regional level, but 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. Lack of coordination through regular contact can lead to communication breakdowns. For example, at one location, FPS, GSA, and tenant agency representatives did not all meet together regularly during a large-scale construction project and surveillance equipment that FPS was responsible for was removed in 2007. During our visit in 2008, FPS officials told us they had not been notified of the action and had not recovered the equipment, but tenant agency representatives maintained there had been coordination with FPS. Furthermore, we found that FPS generally does not share complete BSAs with GSA because FPS believes GSA does not meet the standards under which FPS shares sensitive law enforcement information. GSA security officials maintain that this restriction on their access to security information constrains GSA's ability to protect its buildings and their occupants and is seeking a clarification on access to BSAs as part of the MOA renegotiation with FPS. However, FPS officials told us that they do not intend to change this information sharing procedure during negotiations. We also found that information sharing is constrained when FPS's radios are not interoperable with other law enforcement agencies' radios and FPS cannot communicate directly with the other agencies when responding to incidents. While FPS is taking steps to improve interoperability, it is too soon to tell whether FPS will achieve its goal in accordance with established timelines.

Without greater attention to the key practices, FPS will be ill-equipped to efficiently and effectively fulfill its responsibilities of assessing risk, recommending countermeasures, and sharing information and coordinating with GSA and tenant agencies to secure GSA buildings as the security landscape changes and as new threats emerge. Accordingly, we are making recommendations designed to move FPS toward greater application of key practices and complete implementation of planned improvements. Specifically, the Secretary of Homeland Security should instruct the Director of FPS, in consultation, where appropriate, with other parts of DHS, GSA, and tenant agencies to (1) report regularly to the Secretary on the status of new risk management and countermeasure program activities; (2) develop a methodology and guidance for assessing and comparing the cost-effectiveness of technology alternatives; and (3) work with GSA to determine what information contained in the BSA is needed for GSA to protect buildings and occupants. We provided a draft of the sensitive but unclassified report to DHS and GSA for official review and comment. DHS agreed with our assessment that greater attention to key practices would improve FPS's approach to facility protection and agreed with the report's recommendations. GSA agreed with our findings concerning the challenges that FPS faces in delivering security services for GSA buildings. DHS's comments can be found in appendix II and GSA's comments can be found in appendix III. DHS also provided technical comments that we incorporated, where appropriate.

Background

FPS was created in 1971 and located within GSA until, under the Homeland Security Act of 2002, it was transferred to DHS and placed within ICE, effective March 1, 2003. Under the act, FPS is authorized to protect the buildings, grounds, and property that are under the control and custody of GSA and the persons on the property.[12] FPS is authorized 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. DHS and GSA developed an MOA to set forth roles, responsibilities, and operational relationships between FPS and GSA

[12] 6 U.S.C. § 232 and 40 U.S.C. § 1315. In addition to GSA facilities, the Homeland Security Act of 2002 also provides FPS with the authority to protect the buildings, grounds, and property of other agencies whose functions were transferred to DHS.

concerning the security of GSA buildings. In accordance with the MOA, FPS inspectors[13] are responsible for performing a range of law enforcement and security duties at GSA buildings, including

- patrolling the building perimeter,[14]
- responding to incidents and demonstrations,
- completing risk assessments for buildings[15] and space that GSA is considering leasing,[16]
- recommending countermeasures,
- participating in meetings with GSA property managers and tenant agency representatives, and
- overseeing contract guard operations.[17]

The level of physical protection services FPS provides at each of the 9,000 GSA buildings varies depending on the building's security level. To determine a building's security level, FPS uses the Department of Justice (DOJ) vulnerability assessment guidelines, which categorize federal buildings into security levels I through V based on factors such as building

[13] FPS inspectors are also referred to as Law Enforcement Security Officers. As of April 2009, FPS had 1,236 employees, of whom 694—or 56 percent—were inspectors.

[14] "Patrol" refers to movement within an area for the purpose of observation or surveillance to prevent or detect criminal violations, maintain security, and be available to provide service and assistance to the public.

[15] According to FPS officials, there is no official policy on the number of buildings assigned to each inspector. The number of buildings is entirely dependent on the buildings' geographic dispersion and risk levels.

[16] In accordance with the 2006 MOA between DHS and GSA, FPS is supposed to conduct security assessments—or "prelease assessments"—for proposed buildings that are generally greater than 10,000 square feet. As part of the assessment process, FPS is supposed to inspect the building, identify vulnerabilities, and recommend security countermeasures.

[17] FPS is responsible for overseeing about 15,000 contract guards that provide security services at GSA buildings. FPS inspectors are responsible for conducting contract guard inspections to ensure that guards are in compliance with contract requirements; have up-to-date certifications for required training, including firearms or cardio pulmonary resuscitation training; and are completing assigned duties.

size and number of employees.[18] The DOJ standards recommend minimum security measures for each of the five levels and FPS uses these standards and other information to recommend countermeasures. The DOJ standards also require FPS to complete BSAs[19] every 2 to 4 years, depending on the security level of the building.[20] For example, a BSA is to be completed every 2 years for a level IV building and every 4 years for a level I building. As part of each assessment, the inspector is required to conduct an on-site physical security analysis using FPS's risk assessment tool, known as Federal Security Risk Manager, and interview tenant agency security representatives, GSA realty specialists, site security supervisors, and building managers. After completing their assessments, inspectors make recommendations to GSA and tenant agencies for building security countermeasures,[21] including security equipment[22] and security fixtures.[23] Tenant agencies decide whether to fund countermeasures recommended for security equipment and FPS is responsible for acquiring, installing, and maintaining approved equipment. GSA and tenant agencies determine whether to fund recommended

[18] U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C., June 28, 1995).

[19] A BSA is a type of security evaluation conducted by FPS to determine how susceptible a facility is to various forms of threats or attacks. BSAs include countermeasure recommendations to mitigate threats and reduce vulnerabilities.

[20] On March 10, 2008, ISC issued new standards for determining the security level of federal facilities, which supersede the standards developed in the DOJ's 1995 vulnerability assessment. FPS is currently reassessing building security levels using the updated standards. These standards also change the BSA schedule such that level III, IV, and V buildings will be assessed at least every 3 years, and level I and II buildings will be assessed at least every 5 years. ISC plans to issue updated minimum security countermeasure standards during fiscal year 2009, which FPS intends to implement.

[21] FPS makes two types of countermeasure recommendations: (1) "mandatory" countermeasures are those required to address high risks and ISC minimum security or other nationally recognized security standards or protocols and (2) "optional" countermeasures are those that address moderate or low risks or areas for which minimum ISC standards or other nationally recognized security standards or protocols may not exist.

[22] "Security equipment" refers to security items that are easily removable from the building, such as X-ray machines, magnetometers, closed-circuit television systems and cameras, and intrusion and duress alarm systems.

[23] "Security fixtures" are physical security countermeasures that are part of the building, or are attached to and not easily removable from the building. Examples include vehicle barriers such as bollards, gates, pop-up and arm gates; doors, locks, and card readers at building entrances that serve solely as a locking mechanism; parking lot fencing and gates; guard booths; and blast-resistant windows.

security fixtures and GSA is responsible for acquiring, installing, and maintaining approved fixtures.[24] In some cases, and in accordance with its policies, FPS has delegated the protection of buildings to tenant agencies, which may have their own law enforcement authority or may contract separately for guard services.

FPS is a fully reimbursable agency—that is, its services are fully funded by security fees collected from tenant agencies. FPS charges each tenant agency a basic security fee per square foot of space occupied in a GSA building. In fiscal year 2009, the basic security fee is 66 cents per square foot and covers services such as patrolling the building perimeter, monitoring building perimeter alarms, dispatching law enforcement officers through its control centers, conducting criminal investigations, and performing BSAs. FPS also collects an administrative fee that it charges tenant agencies for building-specific security services, such as controlling access to building entrances and exits and checking employees and visitors. In fiscal year 2009, the fee rate for building-specific expenses is 8 percent. In addition to these security services, FPS provides tenant agencies with additional services upon request, which are funded through reimbursable security work authorizations (SWA) for which FPS charges an administrative fee. For example, tenant agencies fund FPS's security equipment countermeasure recommendations that they approve through SWAs. In fiscal year 2009, the SWA fee rate is 8 percent.

Since transferring to DHS, FPS's mission has expanded beyond solely protecting GSA buildings to include homeland security activities, such as implementing homeland security directives, and providing law enforcement, security, and emergency response services during natural disasters and special events. For example, FPS serves as the sector-specific agency for the Government Facilities critical infrastructure sector under Homeland Security Presidential Directive 7 (HSPD-7).[25]

[24] GSA funds "mandatory" security fixture recommendations and tenant agencies fund "optional" security fixture recommendations through reimbursable work authorizations with GSA.

[25] Issued in 2003, HSPD-7 identified 17 critical infrastructure sectors, which include assets, systems, networks, and functions that provide vital services to the nation. In March 2008, an 18th sector was established—Critical Manufacturing. One of the 18 sectors is the Government Facilities sector which includes a wide variety of facilities owned or leased by federal, state, local, and tribal governments, located domestically and oversees. HSPD-7 designated DHS as the Government Facilities sector-specific agency, and DHS in turn assigned this responsibility to FPS.

Additionally, DHS has authority under the Homeland Security Act to engage FPS in activities DHS deems necessary to enhance homeland security. For example, FPS can be called upon to assist the Federal Emergency Management Agency in responding to natural disasters, and provide backup to other DHS law enforcement units during special events, such as political demonstrations. According to FPS, it is reimbursed for these supportive services.

We have previously identified challenges that raised concerns about FPS's protection of GSA buildings and tenants. In 2004, we reported on the challenges FPS faced in transitioning from GSA to DHS, including issues related to expanding responsibilities and funding.[26] In June 2008, we reported on a range of operational and funding challenges facing FPS.[27] We found that the operational challenges we identified hampered FPS's ability to accomplish its mission of protecting GSA buildings and the actions it took may not have fully resolved the challenges. For example, the number of FPS staff decreased by about 20 percent between fiscal year 2004 and fiscal year 2007. We found that FPS managed these decreases in staffing resources in a way that diminished security and increased the risk of crime and terrorist attacks at many GSA buildings. We further reported that the actions FPS took to address its funding challenges had some adverse implications. For example, during fiscal years 2005 and 2006, FPS's projected expenses exceeded its collections, and DHS had to transfer funds to make up the difference. We also found that although FPS had developed output measures, it lacked outcome measures to assess the effectiveness of its efforts to protect GSA buildings. Moreover, FPS lacked a reliable data management system for accurately tracking performance measures.

As the federal government's landlord, GSA designs, builds, manages, and safeguards buildings to support the needs of other federal agencies. Under the Homeland Security Act of 2002—although FPS was transferred to DHS along with its responsibility to perform law enforcement and related security functions for GSA buildings—GSA also retained some property protection responsibilities. The Homeland Security Act of 2002 stated that:

[26] GAO, *Homeland Security: Transformation Strategy Needed to Address Challenges Facing the Federal Protective Service*, GAO-04-537 (Washington, D.C.: July 14, 2004).

[27] GAO-08-683.

> “Nothing in this chapter may be construed to affect the functions or authorities of the Administrator of General Services with respect to the operation, maintenance, and protection of buildings and grounds owned or occupied by the Federal Government and under the jurisdiction, custody, or control of the Administrator. Except for the law enforcement and related security functions transferred under section 203(3) of this title, the Administrator shall retain all powers, functions, and authorities vested in the Administrator under chapter 1, except section 121(e)(2)(A), and chapters 5 to 11 of Title 40, and other provisions of law that are necessary for the operation, maintenance, and protection of such buildings and grounds.”[28]

In response to a 2005 GAO recommendation[29] and to enhance coordination with FPS, GSA established the Building Security and Policy Division within the Public Buildings Service (PBS)—where FPS once resided—in 2006.[30] This division has three primary branches:

- Building Security Policy—develops GSA security policies.
- Building Security Operations—interfaces with FPS and monitors the services FPS provides to GSA and tenant agencies.
- Physical Security—provides physical security expertise, training, and guidance to GSA leadership, regional staff, and tenant agencies.

During 2006, 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.

[28] 6 U.S.C. § 232.

[29] GAO, *Homeland Security: Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism*, GAO-05-790 (Washington, D.C.: June 24, 2005). In 2005, GAO recommended that GSA establish a mechanism that could serve as a liaison between FPS and tenant agencies, work to address the challenges GSA faces related to security in its buildings, and enable GSA to define its overall role in security following the transfer of FPS to DHS.

[30] PBS, a component within GSA, acquires space on behalf of the federal government through new construction and leasing, and acts as a caretaker for federal properties across the country. PBS is funded primarily through the Federal Buildings Fund, which is supported by rent from federal customer agencies.

In 1995, Executive Order 12977 established the ISC to enhance the quality and effectiveness of security in, and protection of, nonmilitary buildings occupied by federal employees in the United States. ISC has representation from all federal cabinet-level departments and other agencies and key offices, including GSA and FPS.[31] Furthermore, ISC was established as a permanent body to address continuing government security issues for federal buildings. Under the order, ISC became responsible for developing policies and standards, ensuring compliance and overseeing implementation, and sharing and maintaining information. Executive Order 13286 transferred the ISC Chair from GSA to DHS.[32] In 2004, we assessed ISC's progress in fulfilling its responsibilities.[33]

We have identified a set of key facility protection practices from the collective practices of federal agencies and the private sector to provide a framework for guiding agencies' protection efforts and addressing challenges.[34] We focused on the following three key practices for this report: (1) *allocating resources using risk management*; (2) *leveraging technology*; and (3) *information sharing and coordination*. We have used the key practices to evaluate the efforts of the Smithsonian Institution to protect its assets,[35] of DHS to protect its facilities,[36] and of federal entities to protect icons and facilities on the National Mall.[37] Moreover, ISC is

[31] ISC includes representation from the Departments (listed in order of presidential succession) of State, Treasury, Defense, Justice, Interior, Agriculture, Commerce, Labor, Health and Human Services, Housing and Urban Development, Transportation, Energy, Education, Homeland Security, and Veterans Affairs; GSA; the Environmental Protection Agency; the Central Intelligence Agency; and the Office of Management and Budget. Other members of ISC include the Director, U.S. Marshals Service; the Director, Security Policy Board; and the Assistant to the President for National Security Affairs. As a member of ISC, the Department of Defense participates in meetings to ensure that its physical security policies are consistent with ISC security standards and policy guidance, according to the Executive Director of ISC.

[32] Executive Order 13286, dated February 28, 2003, amended numerous executive orders to reflect the transfer of certain functions and responsibilities to the Secretary of Homeland Security. Section 23 of the Executive Order transferred the ISC chair responsibility from GSA to DHS.

[33] GAO-05-49.

[34] GAO-05-49.

[35] GAO-07-1127.

[36] GAO, *National Mall: Steps Identified by Stakeholders Facilitate Design and Approval of Security Enhancements*, GAO-05-518 (Washington, D.C.: June 14, 2005).

[37] GAO-07-658.

using our key facility protection practices as key management practices to guide its priorities and work activities. For example, ISC established subcommittees for technology best practices and training, and working groups in the areas of performance measures and strategic human capital management. ISC also issued performance measurement guidance in 2009.[38]

FPS's Risk Management Approach Is Inadequate, but Improvements Are in Development

FPS is limited in its ability to influence the allocation of resources using risk management because security funding decisions are the responsibility of GSA and tenant agencies. Moreover, FPS uses an outdated risk assessment tool, a subjective approach, and a time-consuming process to conduct BSAs. GSA and tenant agencies have concerns about the quality and timeliness of FPS's risk assessment services and in some cases, are assuming these responsibilities. Although FPS is taking steps to implement a new risk management program, it is unclear when all program components—such as risk assessment tools—will be fully implemented as FPS has extended initial implementation from fiscal year 2009 into fiscal year 2010. FPS's new risk management program could help GSA and tenant agencies refine their resource allocation decisions if risk assessments are enhanced and FPS can help GSA and tenant agencies prioritize risks among all buildings. Until the risk management program is implemented, FPS will continue to use its current approach, which may leave some buildings and tenants vulnerable to terrorist attacks and crime.

FPS's Ability to Influence Resource Allocation Based on Risk is Limited

FPS's ability to influence the allocation of resources based on the results of its risk assessments is constrained because GSA and tenant agencies must agree to fund recommended countermeasures, and we found that tenant agencies were sometimes unwilling to fund recommended security equipment. We have reported that a risk management approach to building protection generally involves identifying potential threats, assessing vulnerabilities, and evaluating mitigation alternatives for their likely effect on risk and their cost.[39] Incorporating information on these elements, a strategy for allocating security-related resources is developed, implemented, and reevaluated over time as conditions change. Through the risk assessment process, FPS inspectors make recommendations for security fixtures and equipment which they include in BSA executive

[38] ISC, *Use of Physical Security Performance Measures*, (Washington, D.C., June 16, 2009).

[39] GAO-05-49.

summaries that FPS is required to share with GSA and tenant agencies. GSA and tenant agencies determine whether to fund recommended security fixtures and GSA is responsible for acquiring, installing, and maintaining approved fixtures. Tenant agencies determine whether to fund recommended security equipment and FPS is responsible for acquiring, installing, and maintaining security equipment. However, tenant agencies may be unwilling to approve FPS's security equipment countermeasure recommendations, in which case FPS views them as choosing to accept the risk. According to officials we spoke with from FPS, GSA, and tenant agencies, tenant agencies may not approve FPS's security equipment countermeasure recommendations for several reasons:

- Tenant agencies may not have the security expertise needed to make risk-based decisions.
- Tenant agencies may find the associated costs prohibitive.
- The timing of the BSA process may be inconsistent with tenant agencies' budget cycles.
- Consensus may be difficult to build among multiple tenant agencies.
- Tenant agencies may lack a complete understanding of why recommended countermeasures are necessary because they do not receive BSAs in their entirety.

For example, in August 2007, FPS recommended a security equipment countermeasure—the upgrade of a surveillance system shared by two locations that, according to FPS officials, would cost around $650,000. While members of one 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. In May 2009, FPS officials 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.[40]

FPS's Current Approach to Risk Management Is Outdated, Subjective, and Time-consuming

Complicating the issue of FPS's limitations in influencing risk-based resource allocation decisions, FPS inspectors use an outdated risk assessment tool, known as Federal Security Risk Manager, to produce BSAs which are also vulnerable to inspector error and subjectivity and can take a considerable amount of time to complete. GSA originally developed the risk assessment tool in the late 1990s when FPS was a part of GSA and updated it in 2002, and it moved with FPS when it was transferred to DHS in 2003. FPS has identified problems with the risk assessment tool and overall approach to developing BSAs, including

- The risk assessment tool contributes to BSA subjectivity because it lacks a rigorous risk assessment methodology. For example, the tool does not incorporate ISC standards or the National Infrastructure Protection Plan (NIPP) framework,[41] therefore, inspectors must apply ISC standards during their reviews of BSAs produced from the risk assessment tool and modify these reports in accordance with the standards.
- Inspectors' compliance with BSA policies and procedures is inconsistent and inspectors must search for risk information from different sources and perform duplicative data entry tasks making it difficult for inspectors to focus fully on the needs of GSA and tenant agencies. Additionally, inspectors record risk assessment findings on paper-based forms and then transfer data to the risk assessment tool and other systems manually, potentially introducing errors during the transfer.

We concur with FPS's findings and also believe the discretion given to inspectors in FPS's risk assessment approach provides less assurance that vulnerabilities are being consistently identified and mitigated. Without consistent application of risk assessment procedures, FPS cannot assure GSA and tenant agencies that expenditures to implement its recommendations are necessary. Furthermore, FPS's reliance on an

[40] GAO-08-683.

[41] The NIPP was founded through HSPD-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.

outdated risk assessment tool provides less assurance that risks and mitigation strategies are adequately identified.

We have previously reported on other concerns about FPS's risk assessment tool.[42] For example, the tool does not allow FPS to compare risks from building to building so that FPS, GSA, and tenant agencies can prioritize security improvements among the nearly 9,000 buildings within GSA's inventory. The ability to compare risks among all buildings is important because it could allow FPS, GSA, and tenant agencies to comprehensively identify and prioritize risks and countermeasure recommendations at a national level and direct resources toward alleviating them. We also reported that the risk assessment tool does not allow FPS to further refine security improvement priorities based on more precise risk categories—rather than the high, medium, or low categories FPS inspectors use under the current system. Furthermore, we reported that the risk assessment tool does not allow FPS to track the implementation status of security recommendations based on assessments.[43] Without this ability, FPS has difficulty determining the extent to which identified vulnerabilities at GSA buildings have been mitigated.

Considering the steps involved, it can also take several months for FPS to complete a BSA. Some of these steps include

- conducting an on-site physical security survey,
- interviewing representatives from GSA and tenant agencies (an inspector may need to visit a site multiple times to meet with all pertinent officials),
- entering survey and interview results into the risk assessment tool and other systems such as the Security Tracking System,
- producing a BSA document that undergoes several layers of review and approval, and
- briefing representatives of tenant agencies and GSA on the BSA results and distributing the executive summary to them.

[42] GAO-07-658.

[43] GAO-08-683.

An FPS supervisory officer told us that it took an average of 3 months to complete a BSA. The officer explained that it may take 2 to 5 weeks for an inspector to complete a security survey, interviews, and a BSA document. The officer gave an example that for one of the buildings within the region, an inspector must interview representatives from 30 tenant agencies. In another example, we found that an FPS inspector had completed a BSA report for one location in April 2008, but at the time of our visit in August 2008 the document was still undergoing supervisory review and tenant agency representatives and GSA had not yet been briefed on the results or received a copy of the executive summary.[44] Furthermore, inspectors are responsible for conducting BSAs for multiple buildings. The inspectors we interviewed were each responsible for conducting BSAs and overseeing security operations at between 1 and 20 buildings.

GSA and Tenant Agencies Are Assuming More Security Responsibilities

GSA security officials at the national and regional levels that we met with were concerned about the quality and timeliness of the risk assessment services that FPS provides. Officials explained that GSA created the current risk assessment tool hastily following the 1995 bombing of the Alfred P. Murrah Federal Building and that FPS inherited a flawed tool when it moved to DHS. GSA security officials expressed concerns over the quality of FPS's BSAs. For example, GSA regional security officials told us that an FPS inspector recommended that GSA remove a structure from a building, because the inspector thought it blocked the view of the security guards. However, according to these officials, FPS had not cited this blocked view as a vulnerability or recommended the structure's removal in previous BSAs, and to their knowledge, there had been no significant changes in identified threats, the space, or the building's tenant composition. GSA security officials also told us that they have had difficulties receiving timely risk assessments from FPS for space that 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. ICE officials told us that there are many occasions where FPS is not notified by GSA of the need for a new lease assessment and in some cases, tenants have moved into leased space

[44] In June 2009, FPS officials told us that tenant agency representatives received the BSA executive summary in October 2008 from FPS and that they would provide the BSA executive summary to the GSA property manager for the campus.

without FPS's knowledge. GSA is updating a tool —the Risk Assessment Methodology Property Analysis and Ranking Tool (RAMPART)[45]—that it began developing in 1998, but has not recently used, to better ensure the timeliness and comprehensiveness of these risk assessments. GSA expects to test and implement the system during fiscal year 2009. GSA security officials told us that they may use RAMPART for other physical security activities, such as conducting other types of risk assessments and determining security countermeasures for new facilities.

The tenant agency officials we spoke with at the five sites did not raise concerns about FPS's risk assessment process, but all of them told us that at the national level, their agencies were taking steps to pursue their own risk assessments for the exterior of their buildings, even though they pay FPS for this service. GSA security officials said they have seen an increase in the number of tenant agencies conducting their own risk assessments. They told us that they are aware of at least nine tenant agencies that are taking steps to acquire risk assessments for the exterior of their buildings. Additionally, we have previously reported that some tenant agencies had told us that they were using or planned to find contractors to complete additional risk assessments because of concerns about the quality and timeliness of FPS's BSAs.[46] We also reported that several DHS components and other tenant agencies were taking steps to acquire their own risk assessments because FPS's assessments were not always timely or adequate. Similarly, we also found that many facilities had received waivers from FPS to enable the agencies to complete their own risk assessments.[47] While 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. However, ICE officials stated that in many cases, the agencies that are pursuing risk assessments are doing so to include both GSA and non-GSA buildings that they occupy, and that in other

[45] The original objective of RAMPART was to implement a risk assessment methodology in software and create a user interface that allowed GSA employees without risk assessment backgrounds to perform and interpret a risk assessment for real property and begin to mitigate risk.

[46] GAO-08-683.

[47] In accordance with FPS's BSA Policy Document (FPS-07-004), some federal agencies with law enforcement or security missions have the personnel and the resources to conduct risk assessments of their own facilities and may not want FPS to conduct a BSA. In these instances, a BSA waiver is completed and signed by the agencies and FPS.

instances, agencies must adhere to other physical security standards and thus conduct their own assessments.

FPS Is Developing a New Risk Assessment Tool and Implementing Updated Security Standards

FPS recognizes the inadequacies of its risk assessment tool, methodology, and process and is taking steps to develop a new risk management program. Specifically, FPS is developing the Risk Assessment and Management Program (RAMP) to improve the effectiveness of FPS's risk management approach and the quality of BSAs. According to FPS, 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 ISC standards, compatible with the risk management framework set forth by the NIPP, and consistent with the business processes outlined in the MOA with GSA. FPS expects that the first phase of RAMP will include BSA and countermeasure management tools, among other functions. 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.[48] According to FPS, RAMP's countermeasure lifecycle management activities will include countermeasure design, review, recommendation, approval, implementation, acceptance, operation, testing, and replacement.

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, it is unclear whether FPS will meet the implementation goals established in the program's proposed timeline. In June 2008, we reported that FPS was going to implement a pilot version of RAMP in fiscal year 2009,[49] but in May 2009, FPS officials told us they intend to implement the first phase in the beginning of fiscal year 2010.

[48] Under RAMP, FPS will use the term, "Facility Security Assessment" instead of BSA.

[49] GAO-08-683.

FPS officials also told us that RAMP training for inspectors will begin in October 2009 and conclude in December 2009. 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. GSA security officials are aware that RAMP's development and implementation have run behind schedule and are concerned about when improvements to FPS's risk assessment processes will be made. Under the 2006 MOA, FPS and GSA recognized that revisions and enhancements would need to be made to the risk assessment process, and FPS agreed it would work in consultation with GSA on any modifications to risk assessment tools. FPS shared RAMP plans with GSA in 2007 and solicited feedback, yet GSA security officials told us they think collaboration could have been stronger and have concerns about RAMP's ability to meet their physical security needs. For example, as stated earlier, GSA relies on FPS to provide it with risk assessments for buildings that it wants to lease, but because FPS does not provide these assessments in a timely manner GSA is taking steps to implement its own risk assessment tool by the end of fiscal year 2009. According to FPS, RAMP will include a risk assessment tool for new lease projects, but it did not include this component in the first development phase and instead, this tool is scheduled for rollout at the end of fiscal year 2010. FPS officials told us that as they move forward with RAMP, they intend to ask GSA and tenant agencies what risk assessment information they need from BSA reports.

Also, FPS officials told us they are reassessing building security levels using ISC's updated facility security level standards[50] and a specialized calculator tool. The updated ISC standards take factors other than a building's size and population into account, including mission criticality, symbolism, threats to tenant agencies, and other factors such as proximity to a major transportation hub.[51] FPS is trying to meet ISC's target date of September 30, 2009, for finalizing updated building security levels for nearly 9,000 GSA buildings. According to FPS, inspectors began reassessing building security levels during June 2008 and as of May 2009, FPS officials told us that inspectors had determined preliminary security levels for all buildings, and finalized security levels for 3,100 buildings.

[50] ISC, *Facility Security Level Determinations for Federal Facilities, an Interagency Security Committee Standard*, (Washington, D.C., Mar. 10, 2008).

[51] ISC officials told us they expect to issue updated standards for physical security countermeasures—which support the updated standards for facility security levels—by the end of fiscal year 2009.

FPS officials told us inspectors have been following ISC guidance in reassessing the facility security levels which require that the tenant agencies make the final security level determination. However, GSA security officials at the national office told us they were receiving feedback from GSA security officials in the regions that some FPS inspectors were presenting the updated security levels as mandatory and final, not as preliminary results to be discussed.

Risk management practices provide the foundation of a comprehensive protection program. Hence, efforts in the other key practice areas—leveraging technology and information sharing and coordination—are diminished if they are not part of a risk management approach which can be the vehicle for using these tools. It is critical that FPS—which is responsible for assessing risk for nearly 9,000 GSA buildings and properties that GSA may lease—replace its outdated, subjective, and time-consuming risk assessment tool and approach with the new program it has been developing since fiscal year 2007, especially as the results of its risk analyses lay the foundation for FPS, GSA, and tenant agencies' security efforts. DHS is the nation's designated leader of critical infrastructure protection efforts; therefore, it is critical that RAMP be developed in an expeditious manner so that DHS can fulfill this mission with regard to federal facilities that FPS protects. Furthermore, department level attention in ensuring that FPS achieves success through regular updates to the Secretary is warranted. This added oversight would enhance the department's ability to monitor RAMP development and make FPS accountable for results, given the delays that RAMP has already experienced.

FPS Lacks a Systematic Approach for Leveraging Technology, but Is Developing a Technology Acquisition Program

FPS's approach to leveraging technology does not ensure that the most cost-effective technologies are being selected to protect GSA buildings. Individual inspectors make technology decisions with limited training and guidance, giving GSA and tenant agencies little assurance that vulnerabilities have been systematically mitigated within and among all buildings as cost-effectively as possible. Although FPS is developing a program for technology acquisition, its implementation has been delayed and it does not include an evaluative component to ensure cost-effectiveness.

Inspectors Have Considerable Latitude in Determining Which Technologies to Pursue, but Receive Little Training and Guidance

As previously discussed, FPS inspectors recommend security fixtures to GSA and security equipment to tenant agencies through the BSA process. However, the training, guidance, and standards that FPS provides to inspectors for selecting technologies are limited. As a result, GSA and tenant agencies have little assurance that the countermeasures inspectors recommend are cost-effective and the best available alternative. We have previously reported that by efficiently using cost-effective technology to supplement and reinforce other security measures, agencies can more effectively apply the appropriate countermeasures to vulnerabilities identified through the risk management process, and that linking the chosen technology to countermeasures identified as part of the risk management process provides assurance that factors such as purpose, cost, and expected performance have been addressed.[52] Furthermore, we have recognized that having a method that allows for cost-effectively leveraging technology to supplement and reinforce other measures represents an advanced application of the key practice.[53]

Through the BSA process, FPS recommends security fixtures to GSA, and GSA has policies and procedures in place to guide its decisions about the recommended investments and to identify and acquire cost-effective fixtures through established contracts with vendors.[54] FPS inspectors also recommend technology-related security equipment through the BSA process and acquire, install, and maintain the security equipment that tenant agencies approve for purchase. FPS does not have a comprehensive approach for identifying, acquiring, and assessing the cost-effectiveness of the security equipment that its inspectors recommend. Instead, individual FPS inspectors identify equipment for its purchase, installation, and maintenance. 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

[52] GAO-05-49.

[53] GAO-05-49.

[54] GSA acquires security fixtures through its Federal Acquisition Service, which procures goods and services for the federal government.

focused on law enforcement.[55] Consequently, inspectors lack recurring technology training. Supervisory officers and inspectors from two of the five sites we visited told us that they learn about security technologies on their own by reviewing industry publications and by attending trade shows and security conferences but inspectors must have the time and funding to attend. A supervisory officer from one FPS region told us the region has sent some inspectors to security conferences sponsored by ASIS International.[56] 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 DOJ minimum countermeasure standards and other relevant ISC standards[57] but these standards do not assist users in selecting cost-effective technologies.

FPS's devolution of responsibility for selecting technology to individual inspectors, whose knowledge of existing and emerging technologies varies because it is built on limited training and personal experience, results in subjective equipment selection decisions. Additionally, the acquisition process can be time-consuming for inspectors—many of whom have other law enforcement and security duties for multiple buildings—because they must search for equipment and vendors and facilitate the establishment of installation and maintenance contracts. FPS's process for acquiring, installing, and maintaining technologies provides GSA and tenant agencies with little assurance that they are getting the highest-quality, most cost-effective technology security solutions and that common vulnerabilities are being systematically mitigated across all buildings. For example, an explosives detection dog was used at one location to screen mail that is distributed elsewhere. 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

[55] According to FPS officials, the design and methodology for its new "Physical Security Refresher Training Program" has been completed and training is scheduled to begin in January 2010.

[56] According to its Web site, ASIS International—an organization that reports having more than 36,000 security industry members—is the preeminent international organization for professionals responsible for security, including managers and directors of security.

[57] Other relevant ISC standards include: (1) ISC Security Design Criteria for new Federal Office Buildings and Major Modernization Projects and (2) Security Standards for Leased Space.

minutes. The GSA regional security officials 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.

FPS Is Developing a Program to Standardize Equipment and Contracting

FPS is 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 explained that the National Countermeasures Program establishes contractual relationships through GSA Schedule 84 to eliminate the need for individual contracting actions when requirements for new equipment or services are identified.[58] FPS officials told us they worked closely with GSA's Federal Acquisition Service (FAS) to develop the program and FAS officials concurred stating, for example, that the two agencies have collaborated to ensure that GSA Schedule 84 has a sufficient number of vendors to support FPS requirements for physical security services. FPS officials said they established an X-ray machine contract through the

[58] GSA Schedule 84 provides agencies with access to a range of established security services and product contracts.

schedule 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. Additionally, FPS officials told us that they participate in the research and development of new technologies with DHS's Science and Technology Directorate.[59]

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. Another concern is that FPS had planned to implement the program throughout fiscal year 2009, but extended implementation into fiscal year 2010 and thus it is not clear whether FPS will meet the program's milestones in accordance with updated timelines. For example, FPS had 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

[59] The Science and Technology Directorate is DHS's primary research and development arm. Its mission is to provide federal, state, and local officials with the technology and capabilities to protect the homeland.

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. FPS had planned to test the program in one region before implementing it nationwide, but after further consideration, FPS management decided to forgo piloting the program in favor of rolling it out nationally. Until the National Countermeasures Program is fully implemented, FPS will continue to rely on individual inspectors to make technology decisions. It would be beneficial for FPS to establish a process for determining the cost-effectiveness of technologies considering the cost and risk implications for the tenant agencies that determine whether they will implement FPS's countermeasure recommendations.

FPS's Information Sharing and Coordination Practices Lack Consistency

FPS, GSA, and tenant agencies share information and coordinate in a variety of ways at the national, regional, and building levels; however, FPS inspectors do not meet regularly with GSA property managers and tenant agencies, FPS and GSA disagree over what threat and risk information should be shared, and FPS faces technical obstacles to communicating directly with other law enforcement agencies when responding to incidents.

Information Sharing and Coordination Practices Have Weaknesses

At the national level, FPS and GSA share information and coordinate in a variety of ways. We have reported that information sharing and coordination among organizations is crucial to producing comprehensive and practical approaches and solutions to address terrorist threats directed at federal buildings.[60] FPS and the Building Security and Policy Division within GSA's PBS hold two biweekly teleconferences—one to discuss building security issues and priorities and the other to discuss the status of GSA contractor security background checks. FPS officials stated that this regular contact with GSA has made their relationship more productive and promotes coordination. GSA security officials also recognize the importance of these teleconferences, although they would like more involvement from FPS such as having better follow-through on meeting action items.

[60] GAO-05-49.

Additionally, FPS and GSA are both members of ISC and serve together on various subcommittees and working groups. The FPS Director and the Director of the PBS Building Security and Policy Division participate in an ISC executive steering committee, which sets the committee's priorities and agendas for ISC's quarterly meetings. These activities could enhance FPS's and GSA's collaboration in implementing ISC's security standards and potentially lead to greater efficiencies. According to FPS and ISC, FPS has consistently participated in ISC working groups, but the staff assigned to some of the groups changed from meeting to meeting. GSA security officials also cited limitations with FPS's staffing of ISC working groups.

FPS and GSA have also established an Executive Advisory Council to enhance the coordination and communication of security strategies, policies, guidance, and activities with tenant agencies in GSA buildings. As the council's primary coordinator, FPS convened the group for the first time in August 2008, and 17 agencies attended. According to FPS, it intends to hold semiannual council meetings, and as of May 2009, FPS had not held a second formal meeting. This council could enhance communication and coordination between FPS and GSA, and provide a vehicle for FPS, GSA, and tenant agencies to work together to identify common problems and devise solutions.

Furthermore, FPS and GSA are renegotiating the 2006 MOA between DHS and GSA to, among other things, improve communication. However, officials told us that this process has been time-consuming and the two parties have different views on the outcomes. FPS and GSA began renegotiating the MOA during fiscal year 2008 and expected to finalize it during fiscal year 2009. However, in May 2009, FPS officials told us they do not have an estimated date for finalizing the MOA and GSA officials told us they do not anticipate reaching an agreement until fiscal year 2010. FPS and GSA recognize that the renegotiation can serve as an opportunity to discuss service concerns and develop mutual solutions. While FPS and GSA concur that the MOA should be used as an accountability tool, FPS thinks the document should offer general guidelines on the services it provides, but GSA wants a more prescriptive agreement.

Overall, FPS and GSA regional officials told us that FPS shares some information with GSA and that collaboration between the two agencies has improved. However, the agencies' satisfaction with this situation differs. The FPS regional officials we spoke with said the agencies' information sharing and coordination procedures work well, while GSA regional security officials told us that communication should be more frequent and the quality of the information shared needs to be improved.

Moreover, according to the GSA officials, FPS's sporadic and restricted sharing of threat information limits GSA's ability to protect its properties. We have reported that by having a process in place to obtain and share information on potential threats to federal buildings, agencies can better understand the risks they face and more effectively determine what preventive measures should be implemented.[61] Additionally, we have reported that sharing terrorism-related information that is critical to homeland security protection is important, and agencies need to develop mechanisms that support this type of information sharing.[62] The 2006 MOA between DHS and GSA requires FPS to provide GSA with quarterly briefings at the regional level. However, GSA regional security officials told us that they were not receiving related threat information as part of these updates until October 2008, when the FPS Director—in response to feedback from GSA—instructed regional personnel to share threat information. The FPS Director advised Regional Directors to meet quarterly with their respective GSA regional administrators, regional commissioners, or security representatives to discuss and share information on regional security issues. The Director further stated that briefings should include unclassified intelligence information concerning threats against GSA buildings and updates to the regional threat assessment, as well as information and analysis on protecting the regions' most vulnerable facilities. Moreover, in its strategic plan,[63] FPS recognizes the importance of ensuring that policies and procedures are being established and followed consistently across the country, and asserts that effective communication between headquarters and regional personnel at all levels will aid in this effort. GSA officials also told us that they are taking steps to replicate headquarters structures in their regions to ensure consistent applications of policies and to standardize communication practices.

While FPS's action to share threat information is a positive step, GSA security officials at the national office told us they received feedback from security staff in the regions that threat briefings were not uniform across regions and varied in their usefulness. The majority of the briefings, the officials said, communicated information about crime incidents and did not, in their view, provide threat information. In May 2009, FPS officials

[61] GAO-05-49.

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

[63] *FPS Strategic Plan: Secure Facilities, Safe Occupants, Fiscal Years 2008 to 2011.*

told us that regions gave briefings during the second quarter of fiscal year 2009, but GSA security officials told us that some regions reported that they had not received these second quarter briefings. To improve information sharing and coordination at the regional level, FPS standardized its quarterly threat briefing format. FPS officials told us that they partnered with GSA to create a sensitive but unclassified (SBU) facility-specific companion document to the BSA called the *"Facility Security Assessment Threat Summary."* According to FPS, this quarterly threat briefing will contain facility-specific information on security performance measures, criminal activity, unclassified intelligence regarding threats, significant events, special FPS law enforcement operations, and potential threats, demonstrations, and other events. FPS officials told us that this quarterly threat briefing format is a positive step in providing a briefing document that GSA can use in evaluating threat information that is germane to its property portfolio. FPS officials told us that they finalized the briefing format and that the Director signed the General Services Administration Threat Briefing Policy directive in June 2009. In contrast, in June 2009, GSA security officials told us that they believe they had little involvement in developing FPS's threat briefing format explaining that although FPS asked GSA to comment on its proposed format—which, according to GSA, it did in March 2009—FPS had not discussed GSA's comments with them or updated GSA on the content or status of the format. GSA security officials told us they have representation on an ISC working group that is developing a standardized design basis threat template to support risk assessment threat ratings.

According to the 2006 MOA, FPS is to meet with GSA property managers and tenant agency representatives when it discusses the results of its BSAs. Depending on the building's security level, the BSA may occur every 2 to 4 years.[64] Apart from these briefings, FPS, GSA, and tenant agencies choose how frequently they will all meet. An information sharing best practice that we have reported on is holding regularly scheduled meetings during which participants can, for example, share security management practices, discuss emerging technologies, and create committees to perform specific tasks, such as policy setting.[65] It is critical that FPS, as the provider of law enforcement and related security services for GSA

[64] Once FPS implements ISC's updated facility security level standards, BSAs will be conducted at least every 3 or 5 years depending on the security level.

[65] GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection,* GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

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. Nevertheless, we identified information sharing gaps at all the sites we visited, and found that in some cases these deficiencies led to decreased security awareness and increased risk.

- At one location, we observed during our interview with the building security committee (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 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.[66]

To improve information sharing and coordination at the building level, FPS and GSA plan to implement ISC's facility security committee standards at all multitenant and single-tenant buildings and campuses after ISC issues them. FPS and GSA could leverage these standards to establish consistent communications and designate the roles and responsibilities of FPS, GSA, and tenant agencies. FPS and GSA have had representation on the ISC working group that is developing the standards. ISC intends to issue the standards in the first quarter of fiscal year 2010, but it is unclear when FPS and GSA will implement them.

GSA security officials also told us that FPS does not consistently or comprehensively inform GSA of changes to services or provide GSA with contingency plans when FPS deploys inspectors and other personnel to provide law enforcement, security, and emergency response services for special events in support of broader homeland security goals. For example, GSA security officials cited some instances in which FPS reduced its services during the 2009 Presidential Inauguration. They noted, for example, that FPS inspectors did not attend BSC meetings and said that FPS did not inform GSA of all service changes. FPS's response to special events and critical incidents is governed by the FPS Interim Critical Incident Response Plan issued by the Director in September

[66] 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.

2007.[67] This plan does not include procedures for notifying GSA and tenant agencies of expected service changes, restrictions, and modifications at the national, regional, and building levels. FPS officials told us that FPS notified tenant agencies in the National Capital Region of expected service changes, restrictions, and modifications during the 2009 inauguration. Officials also said that, when possible, inspectors personally contacted GSA building managers and tenant agency representatives in the region. However, FPS personnel were deployed from all regions in accordance with the critical incident response plan and FPS officials did not tell us that regions other than the National Capital Region were notified. Because GSA and tenant agencies rely on FPS to provide critical law enforcement and security services and tenant agencies pay for these services, we believe it is important for FPS to notify these entities in advance of service changes and provide for interim coverage.

FPS and GSA Disagree Over Sharing Information from the BSA

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 MOA, 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 cited 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 to 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 its buildings and the tenants who occupy them. The BSA executive summary includes

- a brief description of the building;
- an overview of the risk assessment methodology;
- types of threats that the building is exposed to and their risk ratings;

[67] In May 2009, FPS officials told us that FPS's Policy Review Committee and Management-Union Working Group were reviewing the FPS Interim Critical Incident Response Plan and making recommendations regarding a proposed Crisis Response Team Policy.

- countermeasure recommendations, estimated installation and recurring costs; and

- projected threat ratings after countermeasure implementation.

In contrast, a complete BSA includes

- a detailed description of the physical features of the building and its tenants;

- a list of interviewees and contact information;

- a profile of occupants and agency missions;

- recent losses, crimes, and security violations;

- previous security surveys, inspections, and related audits, investigations, and studies;

- descriptions of adequate and inadequate existing countermeasures;

- descriptions of threats and risk ratings;

- descriptions of countermeasure recommendations, and estimated installation and recurring costs; and

- projected threat ratings after countermeasure implementation.

When FPS was housed within GSA and PBS, GSA security officials told us that FPS shared BSAs in their entirety with GSA, but now at the national level, GSA can request full BSAs from FPS, and FPS makes determinations on a case-by-case basis by following and interpreting DHS information sharing policies. However, GSA security officials told us that the process for requesting BSAs is informal and that FPS has not been responsive to these requests overall. Furthermore, considering there are nearly 9,000 buildings in GSA's inventory, this may be an inefficient approach to obtain key facility protection information. We have found that information sharing and coordination are important at the individual building level and that protecting federal buildings requires building security managers to involve multiple organizations to effectively coordinate and share information to prevent, detect, and respond to terrorist attacks.[68]

According to GSA, building protection functions are an integral part of its property preservation, operation, and management responsibilities. In 2000, when FPS was still a part of GSA, Congress considered removing FPS from PBS. At that time, GSA opposed such action asserting that it would divorce security from other federal building functions when security considerations needed to be integrated into decisions about the location, design, and operation of federal buildings. GSA was concerned that separating FPS from PBS would create an organizational barrier between protection experts and PBS asset managers, planners, project managers, and building managers who set PBS budgets and policies for the GSA inventory as a whole and oversaw day-to-day operations in GSA buildings. However, Congress did not remove FPS from PBS, and FPS remained within GSA and PBS until it was transferred to DHS and ICE under the Homeland Security Act of 2002. Prior to the creation of DHS, we expressed concern about separating security from other real property portfolio functions, such as site location, design, and construction for new federal buildings, because decisions on these factors have implications for what types of security will be necessary and effective.[69] We concluded that if DHS was given the responsibility for securing GSA facilities, the role of integrating security with other real property functions would be an important consideration, especially since GSA would still be the caretaker of these buildings.

Under the Homeland Security Act of 2002, FPS was transferred to DHS and retained responsibilities for law enforcement and related security functions for GSA buildings and grounds. However, except for law enforcement and related security functions transferred to DHS, under the act, GSA retained all powers, functions, and authorities in law, related to the operation, maintenance, and protection of its buildings and grounds.[70] As a result of the act, GSA and DHS both have protection responsibilities for GSA-controlled buildings and grounds. DHS and GSA developed an MOA to address roles, responsibilities, and operational relationships

[68] GAO, *National Preparedness:* Technologies to Secure Federal Buildings, GAO-02-687T (Washington, D.C.: Apr. 25, 2002).

[69] GAO, *Building Security: Security Responsibilities for Federally Owned and Leased Facilities*, GAO-03-8 (Washington, D.C.: Oct. 31, 2002).

[70] 6 USC § 203; see also 6 USC § 232.

between FPS and GSA concerning the security of GSA-controlled space. Through this agreement, DHS and GSA determined that FPS would continue to conduct BSAs for GSA. GSA security officials told us that GSA staff at the national, regional, and building levels need the information contained in the BSA to cost-effectively manage their buildings to ensure that they are secure and that their customers, or tenant agencies, are adequately protected. Because GSA personnel do not receive the entire BSA, they must decide on the basis of incomplete information how to use funds to implement countermeasures and mitigate vulnerabilities. Furthermore, GSA property managers are responsible for coordinating and maintaining emergency management plans, such as evacuation and continuity of operations plans, and when a safety or security incident arises at a GSA building, GSA assumes a lead role in the incident command. Without complete risk information, GSA is challenged to maintain appropriate situational awareness and preparedness to protect buildings, especially during emergencies.

Although the Director of FPS recognizes that FPS and GSA have common interests in protecting GSA buildings and the federal employees who work in them, the Director has determined that GSA does not meet the standards under which FPS shares BSAs and maintains that BSA executive summaries provide GSA with sufficient information. FPS designates the SBU information contained in BSAs as "law enforcement sensitive" (LES)[71] in accordance with DHS and ICE policies. FPS considers the BSA to be an LES document because it incorporates all aspects of a location's physical security into one document whose release outside of the law enforcement arena could adversely impact the conduct of law enforcement programs. According to FPS, the BSA can include LES information such as:

- information, details, or criminal intelligence data indicating why a threat is deemed credible;
- information and details relating to any ongoing criminal investigations, law enforcement operations, or both; and
- detailed analysis of why the lack or inadequacy of a countermeasure creates an exploitable vulnerability.

[71] According ICE policy, LES information is a type of SBU information that is compiled for law enforcement purposes, the unauthorized disclosure of which could adversely impact the conduct of law enforcement programs or the privacy or welfare of involved persons.

According to FPS, LES information is safeguarded and determinations to disseminate LES information are made in accordance with a DHS information safeguarding management directive[72] and an ICE directive for safeguarding LES information.[73] FPS maintains that GSA does not need to know the LES information that is contained in the BSA and that if the BSA is released to GSA, the risk of unscrupulous or criminal use of the information would increase significantly. According to FPS, the information contained in the BSA is not critical to GSA's performance of its authorized, assigned mission. FPS further maintains that GSA retains no legal responsibility for the physical protection and law enforcement operations within GSA buildings because the Homeland Security Act of 2002 transferred FPS's law enforcement and related security functions from GSA to DHS and that under the act it is responsible for protecting the buildings, grounds, and property under GSA's control or custody.

We have reported on the importance of sharing terrorism-related information that is critical to homeland security protection and have identified a need for agencies to develop mechanisms that support this information sharing.[74] Other federal agencies have found ways to share sensitive information with other entities. For example, in response to a GAO recommendation,[75] the Transportation Security Administration established regulations that allow for sharing sensitive security information with persons covered by the regulations who have a need to know, including airport and aircraft operators, foreign vessel owners, and Transportation Security Administration employees.[76] The ICE directive for safeguarding LES information states that an information sharing and access agreement in the form of a memorandum of understanding or agreement may formalize LES information exchanges between DHS and an external entity. Moreover, according to standard language in FPS's BSAs, a security clearance is not required for access to LES information; a

[72] DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified Information.*

[73] ICE Directive 73003.1, *Safeguarding Law Enforcement Sensitive Information.*

[74] GAO-05-207.

[75] GAO, *Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information*, GAO-05-677 (Washington, D.C.: June 29, 2005).

[76] GAO, *Transportation Security Administration's Processes for Designating and Releasing Sensitive Security Information*, GAO-08-232R (Washington, D.C.: Nov. 30, 2007).

criminal history check and a national fingerprint check—performed in accordance with Homeland Security Presidential Directive 12 (HSPD-12)[77] investigative requirements—is required. According to GSA, it follows these requirements. Moreover, GSA has an information safeguarding policy in place to protect SBU building information which can include:

- the location and details of secure functions or space in a building such as secure routes for prisoners and judges inside courthouses;
- the location and details of secure functions or secure space such as security and fire alarm systems;
- the location and type of structural framing for the building including any information regarding structural analysis, such as counterterrorism methods used to protect the building and occupants; and
- risk assessments and information regarding security systems or strategies of any kind.[78]

In the 2006 MOA, FPS and GSA agreed that shared SBU information would be handled in accordance with each agency's information safeguarding policies. Furthermore, one of FPS's strategic goals is to foster relationships to increase the proactive sharing of information and intelligence. In its strategic plan, FPS states that it will use efficient information sharing and information protection processes based on mutually beneficial, trusted relationships to ensure the implementation of effective, coordinated, and integrated infrastructure protection programs and activities.[79]

When we spoke with FPS and GSA officials in 2008, they thought the MOA renegotiation could serve as a platform for determining what BSA information should be shared. However, when we spoke with FPS and

[77] HSPD-12 is the policy for a common identification standard for federal employees and contractors. Its purpose is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors.

[78] PBS 3490.1A *Document Security for Sensitive But Unclassified Building Information* (June 1, 2009). This document cancelled PBS 3490.1 *Document Security for Sensitive But Unclassified Paper and Electronic Building Information* (Mar. 8, 2002).

[79] *FPS Strategic Plan, Secure Facilities, Safe Occupants, Fiscal Years 2008 to 2011.*

GSA officials in 2009, they did not know when the MOA would be renegotiated and FPS determined it would not change BSA sharing procedures during the renegotiation. Therefore, GSA will continue to receive BSA executive summaries and the individual BSAs that FPS approves for sharing, but it will not have access to other BSA information that it could use to make risk-based decisions to protect its buildings, the federal employees who work in them, and visitors to these buildings.

In a post-September 11 era, it is crucial that federal agencies work together to share information to advance homeland security and critical infrastructure protection efforts. Information is a crucial 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 significant challenges faced in this area[80]—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. GSA raises strong arguments for having this information and FPS could do more to resolve this situation.

FPS's and Other Law Enforcement Organizations' Communication Systems Lack Interoperability

FPS provides the law enforcement response for incidents at GSA buildings, during which it may need to communicate with other first responders. Additionally, DHS can call upon FPS to provide law enforcement and security services at natural disasters or special events such as political demonstrations, and FPS must then communicate with other federal, state, and local first responders. For these situations, having an interoperable communication system is desirable. However, first responders continue to use various, and at times incompatible, communications technologies, making it difficult to communicate with neighboring jurisdictions or other first responders to carry out the response. We noted during our review that FPS radios lack

[80] GAO-05-207.

interoperability, meaning they are unable to communicate with the equipment used by other law enforcement agencies—federal, state, and local. Delayed communications with area first responders during emergencies could curtail the timeliness and effectiveness of FPS's law enforcement services.

- FPS officials at one location told us that only new FPS vehicles have had radio upgrades, some FPS personnel have new hand-held radios, and other handheld radios have not been changed in 6 years. Changes in radio technology can inhibit interoperability among first responders who upgrade equipment as possible.

- FPS officials at one location told us that FPS can use the same radio frequency as the local police department, but the two organizations' radio systems are not fully interoperable because the police use a digital system and FPS does not. Therefore, communication between these entities can be limited.

- FPS officials at one location told us that federal and local law enforcement agencies communicate with FPS via telephone or through the area FPS MegaCenter,[81] instead of directly through radios, because the organizations' radio systems are not interoperable. Therefore, communication among these entities can be limited.

- FPS officials at one location told us that FPS's handheld radios are not interoperable with those of area federal and local law enforcement personnel, because FPS does not use the same radio band spectrum other federal law enforcement agencies use and instead uses its own ultra-high-frequency band. As a result, communication among these entities is limited.

- FPS officials at one location told us that their radios are not interoperable with those of the local police department. Therefore, communication between the two entities can be limited. FPS is exploring whether it can connect to the police department through a local interagency communications system.

FPS is developing a National Radio Program that includes a component intended to make FPS's radios interoperable with those of other federal,

[81] FPS MegaCenters provide three primary security services—alarm monitoring, radio monitoring, and dispatching of FPS and contract guards.

state, and local law enforcement organizations. FPS began planning this initiative in 2008, was working to fill the program manager position by the end of June 2009, and expects to achieve full implementation by 2013. According to FPS officials, they have established a branch under the FPS MegaCenter program specifically dedicated to enhancing and supporting the National Radio Program. Consistent with establishing this new branch, FPS officials said they are working to fill contract positions in each region for radio technicians to support the technical requirements associated with mobile radios, portable radios, programming, and the radio network infrastructure. According to FPS, they are working to contract for a survey and design team to coordinate with FPS's regional offices, the National Radio Program, and the MegaCenter program to standardize and enhance the national radio infrastructure.

According to FPS officials, the enhancements to FPS's communications will provide solutions for newer technologies and will meet national communications standards and DHS standards for advanced encryption. FPS officials said they are beginning an internal evaluation of FPS's existing communications capabilities, which should allow future enhancement efforts to be prioritized as part of an overall effort to enhance national radio coverage. FPS officials said they are working to procure, program, and issue more than 2,900 new radios that conform to new equipment standards and will eventually phase out older equipment used by FPS officers and guards. FPS officials said that all future radios issued will conform to updated standards to promote uniformity and enhanced support capabilities. While FPS officials think interoperability will be improved under this initiative, they cautioned that their law enforcement counterparts' communication equipment must meet DHS's advanced encryption standard which can be a challenge for state and local partners.

Conclusions

FPS has a number of improvements planned or in development that, if fully incorporative of the key practices, will provide greater assurance that FPS is effectively protecting GSA buildings and maximizing security investment dollars. The key practices we examined vis-à-vis FPS—allocating resources using risk management, leveraging technology, and information sharing and coordination—are critical components to an effective and efficient physical security program. However, FPS's application of these practices had limitations and as a result, there is a lack of assurance that federal buildings under the control and custody of GSA, the employees who work in them, and visitors to them are being adequately protected. Related to allocating resources using risk management, FPS's assessment of risks at buildings is a critical responsibility considering the results lay the foundation by which GSA and tenants make resource allocation decisions. However, FPS's current risk assessment process is inadequate and its efforts to improve it through the development of RAMP have been delayed. Related to leveraging technology, planned improvements to the way inspectors acquire security equipment through the National Countermeasures Program have also experienced delays and knowing the cost implications of different alternatives is the foundation of this key practice, although FPS is not directly addressing this critical element. Continued delays in the implementation of improvements in these critical areas—risk management and leveraging technology—are of concern and deserving of greater attention by DHS management. Furthermore, related to information sharing and coordination, FPS's communications with GSA and tenants could benefit from more clearly defined parameters for consistency, frequency, and content, and issues related to interoperability with other law enforcement agencies surfaced as a concern that FPS is trying to address. Without a greater focus on the key practices, FPS will be ill-equipped to sufficiently manage security at GSA buildings, and assist with broader homeland security efforts as the security landscape changes and new threats emerge.

Recommendations for Executive Action

We are making three recommendations to the Secretary of Homeland Security aimed at moving FPS toward greater use of the key practices we assessed. Specifically, we recommend that the Secretary instruct the Director of FPS, in consultation, where appropriate, with other parts of DHS, GSA, and tenant agencies to take the following three actions:

1. Provide the Secretary with regular updates, on a mutually agreed-to schedule, on the status of RAMP and 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.

2. In conjunction with the National Countermeasures Program, develop a methodology and guidance for assessing and comparing the cost-effectiveness of technology alternatives.

3. 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 SBU 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 regularly on a mutually agreed-to schedule.

Agency Comments and Our Evaluation

We provided a draft of the sensitive but unclassified report to DHS and GSA for review and comment. DHS agreed with our assessment that greater attention to key practices would improve FPS's approach to facility protection and agreed with the report's recommendations. Furthermore, DHS stated that FPS will continue to work with key stakeholders to address other security issues that were cited in our report, for which specific recommendations were not made. With respect to the first recommendation—to provide the Secretary of Homeland Security with regular updates on the status of RAMP and the National Countermeasures Program—DHS stated that FPS will submit a consolidated monthly report to the Secretary.

Although DHS agreed with our second and third recommendations, we are concerned that the steps it described are not comprehensive enough to address the intent of the recommendations. For the second recommendation—to develop a methodology and guidance for assessing and comparing the cost-effectiveness of technology alternatives—DHS commented that such efforts will be a part of FPS's development of RAMP and that future phases of RAMP will include the ability to evaluate countermeasure alternatives based on cost and the ability to mitigate identified risks. However, RAMP has experienced delays and it is unclear when this future component of RAMP will be developed and implemented. Moreover, as we reported, FPS inspectors have considerable latitude in determining which technologies and other countermeasures to recommend, but receive little guidance to help them assess the cost-effectiveness of these technologies. Until the cost-analysis component of RAMP is implemented, it will be important for inspectors to have guidance they can use to make cost-effective countermeasure recommendations so that GSA and tenant agencies can be assured that their investments in FPS-recommended technologies and other countermeasures are cost-effective, consistent across buildings, and the best available alternatives.

Regarding the third recommendation—to reach consensus with GSA on what information contained in the BSA is needed for GSA to fulfill its protection responsibilities and to establish information sharing and safeguarding procedures—DHS responded that FPS is developing a facility security assessment template as a part of RAMP to produce reports that can be shared with GSA and other agencies. However, 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. As we reported, FPS and GSA fundamentally disagree over what BSA information should be shared and FPS has decided not to discuss this matter with GSA as part of the MOA renegotiation. Furthermore, RAMP continues to experience delays and it is unclear when it will produce facility security assessments than can be shared with GSA. 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.

GSA agreed with our findings concerning the challenges that FPS faces in delivering security services for GSA buildings. GSA indicated that it will continue to work closely with FPS to ensure the protection of GSA buildings, their tenants, and visitors to these buildings. GSA stated that it will work with FPS to address our recommendation that the two agencies reach a consensus on the sharing and safeguarding of information contained in BSAs. DHS also provided technical comments, which we incorporated where appropriate. DHS's comments can be found in appendix II and GSA's comments can be found in appendix III.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Acting Administrator of General Services, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions about this report, please contact me at (202) 512-2834 or goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Sincerely yours,

Mark L. Goldstein
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

The objective of this report was to determine whether the Federal Protective Service's (FPS) approach to security for buildings under the control and custody of the General Services Administration (GSA) reflects key facility protection practices. Through previous work, we identified a set of key practices from the collective practices of federal agencies and private sector entities that can provide a framework for guiding agencies' protection efforts and addressing challenges.[1] These key practices form the foundation of a comprehensive approach to building protection. We used our key facility protection practices as criteria to evaluate the steps that FPS has taken. We used the following key practices as criteria: allocating resources using risk management; leveraging technology; and information sharing and coordination. For the purposes of this review, we did not consider three other key practices for varying reasons: performance measurement and testing, because we reported on the limitations FPS faces in assessing its performance in 2008; aligning assets to mission, because GSA, not FPS, controls the asset inventory; and strategic management of human capital, because we are currently reviewing FPS's management of human capital.

To examine FPS's application of key practices at the building level, we selected five sites, basing our selection on factors that included geographical diversity, high occupancy, the building's designated security level, other potential security considerations such as new or planned building construction, and recent and ongoing work. Selected sites included three multitenant level IV buildings,[2] one single-tenant level IV campus, and one single-tenant level III campus.[3]

Collectively, the sites we selected illustrate the range of building protection practices applied by FPS. At each site, we interviewed FPS, GSA, and tenant agency officials with primary responsibility for security

[1] 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).

[2] At the time of our review, a level IV facility had over 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.

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

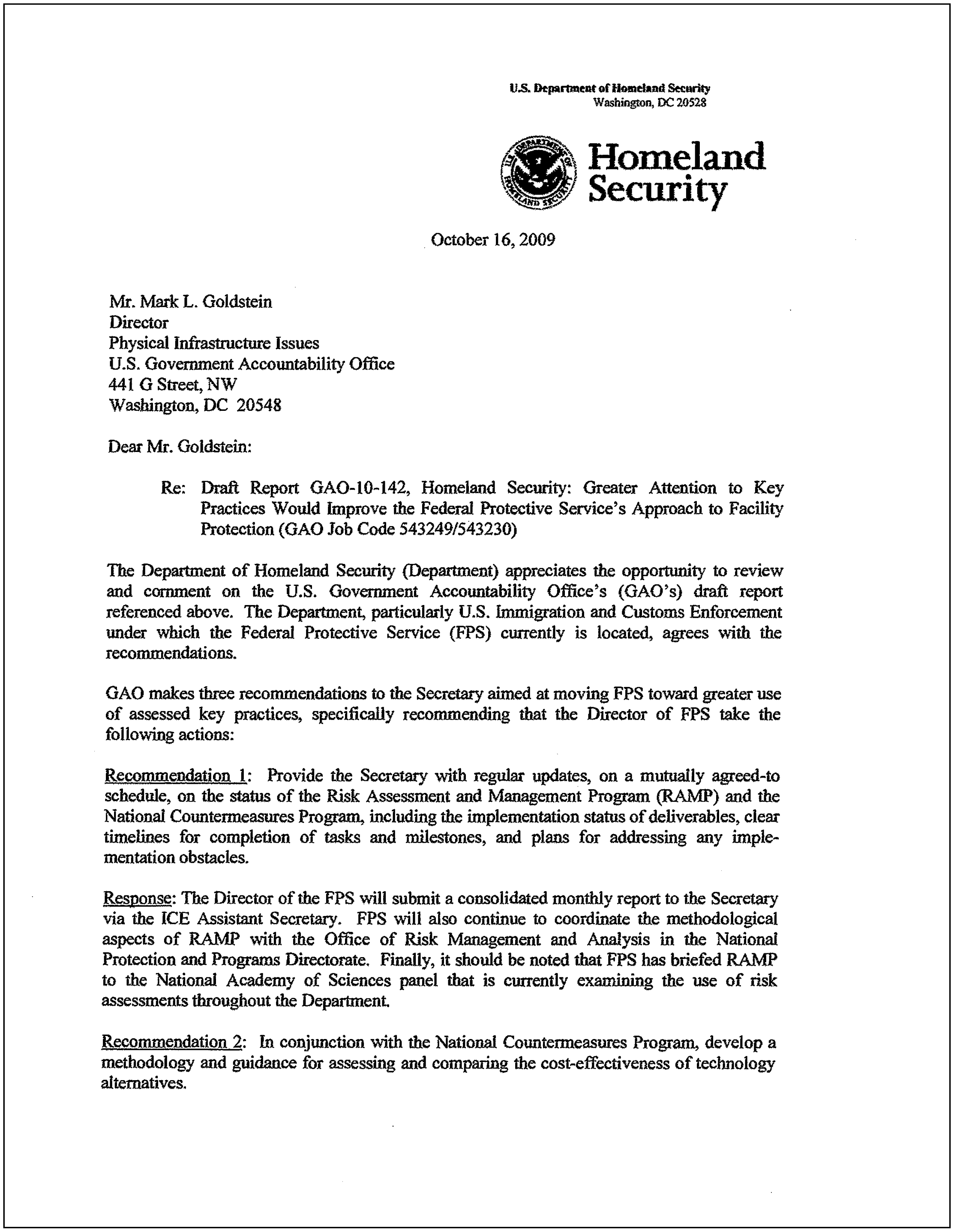
implementation, operation, and management. We toured each site and observed the physical environment, the buildings, and the principal security elements to gain firsthand knowledge of the building protection practices. We collected documents, when available, that contained site-specific information on security risks, threats, budgets, and staffing for analysis. Because we observed FPS's efforts to protect GSA buildings at a limited number of sites, our observations cannot be generalized to all the buildings that FPS is responsible for securing. To supplement these site visits, we interviewed FPS and GSA security officials from the four regions where we had visited buildings—regions 2, 4, 7, and 11. We also interviewed FPS and GSA security officials at the national level and collected supporting documentation on security plans, policies, procedures, budgets, and staffing for analysis. For example, we reviewed the 2006 Memorandum of Agreement between the Department of Homeland Security (DHS) and GSA that sets forth the security responsibilities of FPS and GSA at federal buildings. We also interviewed the executive director of the Interagency Security Committee (ISC), and we analyzed ISC's *Facility Security Level Determinations for Federal Facilities*, *Security Design Criteria for new Federal Office Buildings and Major Modernization Projects*, *and Security Standards for Leased Space*. We also analyzed the facility security level standards and minimum security requirements set forth by the Department of Justice's (DOJ) *DOJ Vulnerability Assessment of Federal Facilities*.[4] We analyzed FPS planning documents, including FPS's 2008-2011 Strategic Plan and the Risk Assessment and Management Program Concept of Operations. We analyzed laws that described FPS and GSA's protection authorities including the Homeland Security Act of 2002, and Title 40 of the United States Code. We also analyzed laws and internal documents that govern FPS's information safeguarding practices including DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified Information* and ICE Directive 73003.1, *Safeguarding Law Enforcement Sensitive Information.*

We conducted this performance audit from January 2008 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

[4] The U.S. Department of Justice, *DOJ Vulnerability Assessment of Federal Facilities* (Washington, D.C.: June 28, 1995).

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 16, 2009

Mr. Mark L. Goldstein
Director
Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Goldstein:

Re: Draft Report GAO-10-142, Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection (GAO Job Code 543249/543230)

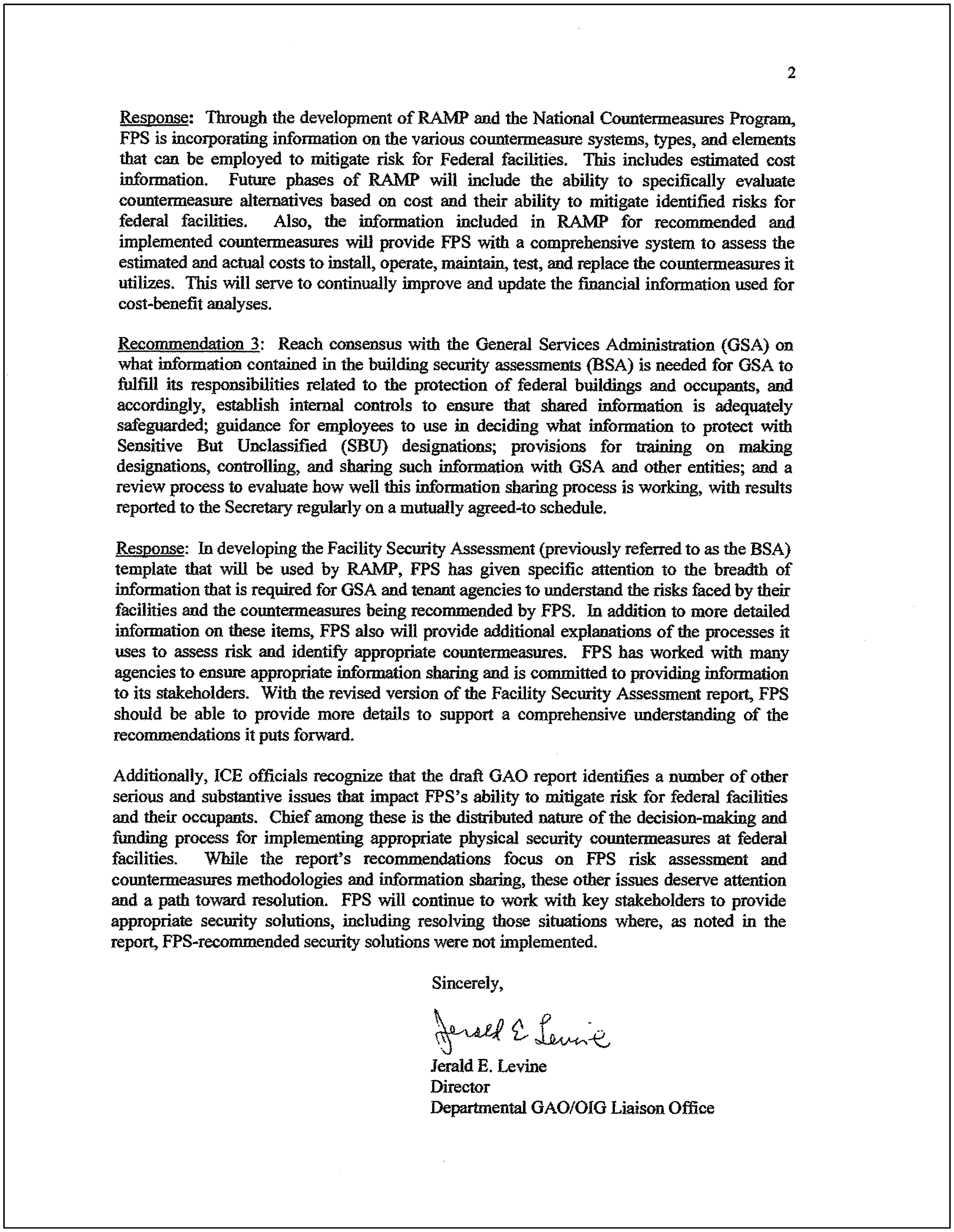
The Department of Homeland Security (Department) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report referenced above. The Department, particularly U.S. Immigration and Customs Enforcement under which the Federal Protective Service (FPS) currently is located, agrees with the recommendations.

GAO makes three recommendations to the Secretary aimed at moving FPS toward greater use of assessed key practices, specifically recommending that the Director of FPS take the following actions:

Recommendation 1: Provide the Secretary with regular updates, on a mutually agreed-to schedule, on the status of the Risk Assessment and Management Program (RAMP) and 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.

Response: The Director of the FPS will submit a consolidated monthly report to the Secretary via the ICE Assistant Secretary. FPS will also continue to coordinate the methodological aspects of RAMP with the Office of Risk Management and Analysis in the National Protection and Programs Directorate. Finally, it should be noted that FPS has briefed RAMP to the National Academy of Sciences panel that is currently examining the use of risk assessments throughout the Department.

Recommendation 2: In conjunction with the National Countermeasures Program, develop a methodology and guidance for assessing and comparing the cost-effectiveness of technology alternatives.



Response: Through the development of RAMP and the National Countermeasures Program, FPS is incorporating information on the various countermeasure systems, types, and elements that can be employed to mitigate risk for Federal facilities. This includes estimated cost information. Future phases of RAMP will include the ability to specifically evaluate countermeasure alternatives based on cost and their ability to mitigate identified risks for federal facilities. Also, the information included in RAMP for recommended and implemented countermeasures will provide FPS with a comprehensive system to assess the estimated and actual costs to install, operate, maintain, test, and replace the countermeasures it utilizes. This will serve to continually improve and update the financial information used for cost-benefit analyses.

Recommendation 3: Reach consensus with the General Services Administration (GSA) on what information contained in the building security assessments (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 (SBU) 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 regularly on a mutually agreed-to schedule.

Response: In developing the Facility Security Assessment (previously referred to as the BSA) template that will be used by RAMP, FPS has given specific attention to the breadth of information that is required for GSA and tenant agencies to understand the risks faced by their facilities and the countermeasures being recommended by FPS. In addition to more detailed information on these items, FPS also will provide additional explanations of the processes it uses to assess risk and identify appropriate countermeasures. FPS has worked with many agencies to ensure appropriate information sharing and is committed to providing information to its stakeholders. With the revised version of the Facility Security Assessment report, FPS should be able to provide more details to support a comprehensive understanding of the recommendations it puts forward.

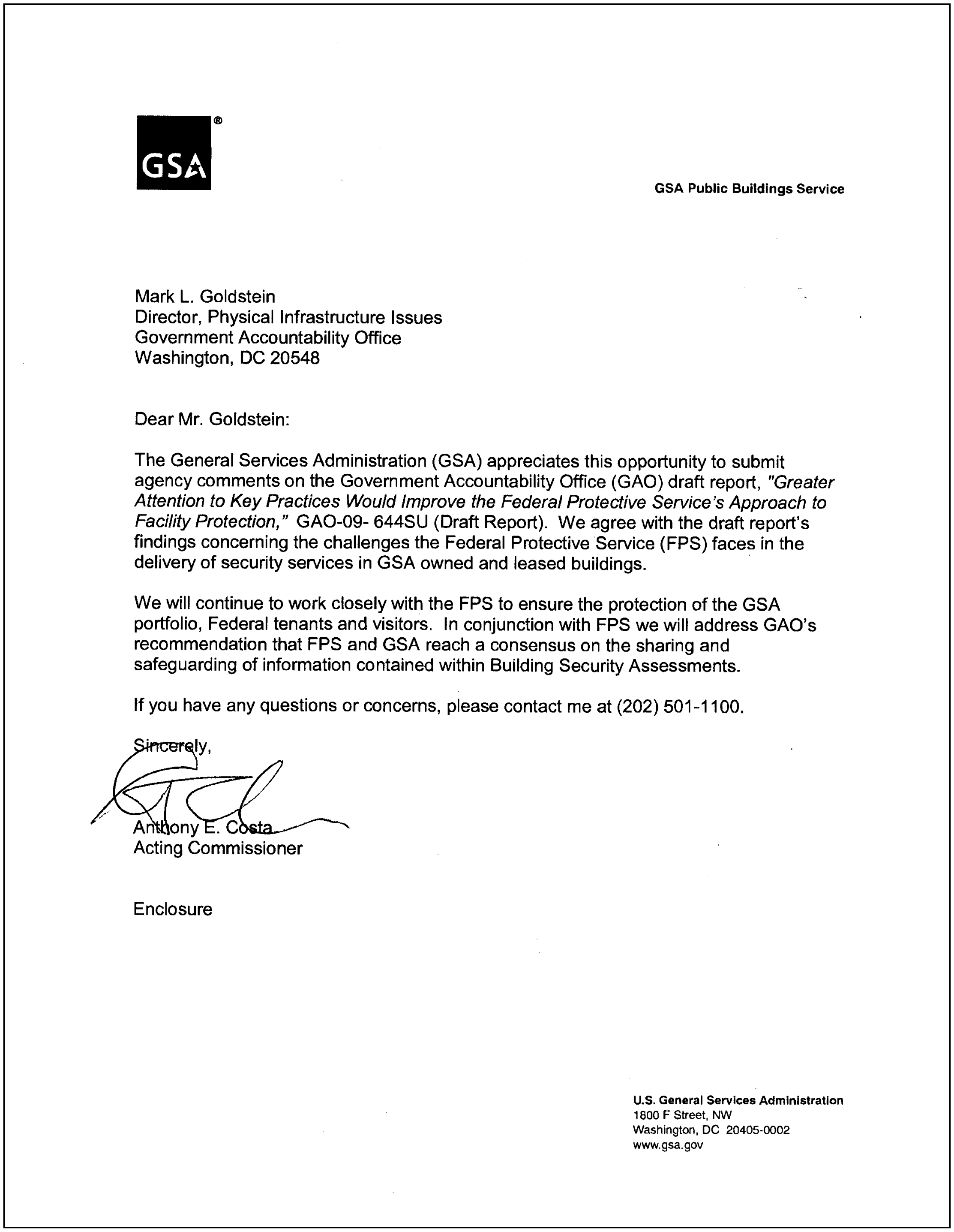
Additionally, ICE officials recognize that the draft GAO report identifies a number of other serious and substantive issues that impact FPS's ability to mitigate risk for federal facilities and their occupants. Chief among these is the distributed nature of the decision-making and funding process for implementing appropriate physical security countermeasures at federal facilities. While the report's recommendations focus on FPS risk assessment and countermeasures methodologies and information sharing, these other issues deserve attention and a path toward resolution. FPS will continue to work with key stakeholders to provide appropriate security solutions, including resolving those situations where, as noted in the report, FPS-recommended security solutions were not implemented.

Sincerely,

Jerald E Levine

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: Comments from the General Services Administration



GSA Public Buildings Service

Mark L. Goldstein
Director, Physical Infrastructure Issues
Government Accountability Office
Washington, DC 20548

Dear Mr. Goldstein:

The General Services Administration (GSA) appreciates this opportunity to submit agency comments on the Government Accountability Office (GAO) draft report, *"Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection,"* GAO-09- 644SU (Draft Report). We agree with the draft report's findings concerning the challenges the Federal Protective Service (FPS) faces in the delivery of security services in GSA owned and leased buildings.

We will continue to work closely with the FPS to ensure the protection of the GSA portfolio, Federal tenants and visitors. In conjunction with FPS we will address GAO's recommendation that FPS and GSA reach a consensus on the sharing and safeguarding of information contained within Building Security Assessments.

If you have any questions or concerns, please contact me at (202) 501-1100.

Sincerely,

Anthony E. Costa
Acting Commissioner

Enclosure

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Mark L. Goldstein, (202) 512-2834 or goldsteinm@gao.gov

Staff Acknowledgments

In addition to the contact named above, David Sausville, Assistant Director; Denise McCabe, Analyst-in-Charge; Anne Dilger; Elizabeth Eisenstadt; Brandon Haller; Robin Nye; Susan Michal-Smith; and Adam Yu made key contributions to this report.

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