United States Government Accountability Office

Report to the Ranking Member, Committee on Homeland Security, House of Representatives

March 2015

HOMELAND SECURITY

Actions Needed to Better Manage Security Screening at Federal Buildings and Courthouses

Accessible Version

GAO-15-445

March 2015

HOMELAND SECURITY

Actions Needed to Better Manage Security Screening at Federal Buildings and Courthouses

GAO Highlights

Highlights of GAO-15-445, a report to the Ranking Member, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

FPS and USMS conduct building security screening at thousands of GSA buildings across the country. Given continued concerns related to the security of federal buildings, GAO was asked to examine the: (1) challenges federal entities face in their efforts to prevent prohibited items and individuals who may pose a security threat from entering GSA buildings and (2) actions federal entities have taken to assess the effectiveness of their screening efforts, and the results of those actions. GAO conducted site visits to 11 selected buildings in three metropolitan areas based on a variety of criteria, including security level, agency officials' recommendations, and for FPS, possible inconsistencies in its data on prohibited items, and other factors. GAO analyzed FPS's and USMS's data, reviewed relevant documentation, and interviewed FPS and USMS officials in headquarters and the field.

What GAO Recommends

GAO recommends that FPS and USMS each develop and implement a strategy for using covert and intrusion testing, and prohibited-items data to improve security-screening efforts. Specifically, for FPS, the strategy would, among other things, help determine which covert testing scenarios to use. For USMS, the strategy would, among other things, help determine the appropriate frequency of intrusion testing. DHS and DOJ concurred with GAO's recommendations.

View GAO-15-445. For more information, contact Mark L. Goldstein at (202) 512-2834 or GoldsteinM@gao.gov.

What GAO Found

The Department of Homeland Security's (DHS) Federal Protective Service (FPS) and the Department of Justice's (DOJ) United States Marshals Service (USMS) experience a range of challenges in their efforts to provide effective security screening, including:

- *Building characteristics and location may limit security options*: many General Services Administration (GSA) buildings were designed and constructed before security screening became a priority.
- *Balancing security and public access*: striking an appropriate balance between facilitating the public's access to government services and providing adequate security can be difficult, for example, when there is a high volume of visitors.
- *Operating with limited resources*: some FPS protective security officers are not fully trained to conduct security screening, and FPS and USMS may have limited funding for additional training or additional security officers.
- *Working with multiple federal tenants*: many tenant stakeholders at multi-tenant GSA buildings have differing needs and priorities that may not always align when trying to build consensus for security-screening decisions.
- *Effectively informing the public of prohibited items*: prohibited items vary by building, and some signage did not effectively relay information to the public.

To assess security-screening efforts, both FPS and USMS have taken steps such as conducting covert and intrusion tests and collecting data on prohibited items. From fiscal years 2011 to 2013, FPS data show that protective security officers passed covert tests on security-screening procedures at a low rate. In October 2012, FPS reduced the number of screening scenarios used for covert testing, but has since reinstated some of them. USMS data show that court security officers passed intrusion tests on security screening at a higher rate. For example, USMS reported that court security officers passed 83 percent of intrusion tests on security screening in fiscal year 2010, 91 percent in fiscal year 2011, and 92 percent in fiscal years 2012 and 2013. Although USMS tests more frequently than FPS, it has not met its intrusion-test frequency requirement per building each year. In addition, FPS's and USMS's data on prohibited items show wide variations in the number of items identified across buildings. For example, FPS reported it had detected approximately 700,000 prohibited items in 2013; however, FPS data showed that there were 295 buildings with no reported data on prohibited items from fiscal years 2004 through 2013. While FPS and USMS may use the results of covert and intrusion tests to address problems at the individual building or FPS region or USMS district level, to some degree, they do not use the results to strategically assess performance nationwide. The benefits of using data in this manner are reflected in the Interagency Security Committee's (ISC) guidance, as well as key practices in security and internal control standards GAO has developed. Without a more strategic approach to assessing performance, both FPS and USMS are not well positioned to improve security screening nationwide, identify trends and lessons learned, and address the aforementioned challenges related to screening in a complex security environment.

Contents

Figures

Abbreviations

AOUSC	Administrative Office of the United States Courts
DHS	Department of Homeland Security
DOJ	Department of Justice
FPS	Federal Protective Service
FSL	facility security level
GSA	General Services Administration
ISC	Interagency Security Committee
SSA	Social Security Administration
USCIS	United States Citizenship and Immigration Services
USMS	U.S. Marshals Service

Letter

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

March 31, 2015

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

Dear Mr. Thompson:

Federal buildings continue to be targets of terrorist attacks and other acts of violence, as evidenced by high-profile domestic events such as the 2013 shooting at the Washington Navy Yard in Washington, D.C.; the terrorist attacks of September 11, 2001; and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. These incidents highlight the importance of protecting the over 1-million government employees who work in, as well as the public who visits the over 8,900 buildings in the United States that are held or leased by the General Services Administration (GSA). As recently as late October 2014, the Federal Protective Service (FPS) took actions designed to enhance its presence and security at various federal buildings it protects in light of recent world events targeting government personnel and buildings. FPS, a subcomponent of the National Protection and Programs Directorate within the Department of Homeland Security (DHS), is the primary agency responsible for protecting federal buildings. The United States Marshals Service (USMS), a component of the Department of Justice (DOJ), has primary physical security responsibility for federal courthouses. Securing federal real property continues to be a challenge for agencies and is among the major reasons GAO designated federal real property management as a high-risk area.[1]

Screening for prohibited items[2] and individuals who may pose a security threat is a focal point of the day-to-day security operations at federal buildings. FPS protective security officers and USMS court security

[1]GAO, *High Risk Series: An Update,* GAO-13-283 (Washington, D.C.: Feb. 2013).

[2]The Interagency Security Committee (ISC) defines a prohibited item as an item, legal or illegal in nature, where possession is restricted from entry into a facility by federal, state, or local law, regulation, court order, rule, or facility security committee policy. ISC, *Items Prohibited from Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: February 2013).

officers are security guards contracted to provide various security functions at federal buildings. These officers are generally the first contact with federal agencies for individuals entering federal buildings and courthouses. Protective security officers and court security officers are primarily responsible for controlling access to these federal buildings by checking the identification of government employees and visitors and operating security equipment, such as x-ray machines and walk-through magnetometers, to screen for and prevent the entry of prohibited items including illegal items such as firearms.

Given continued concerns related to the security of federal buildings, you requested that we examine the effectiveness of FPS's and USMS's efforts to prevent prohibited items and individuals who may pose a security threat from entering GSA buildings. Specifically, this report examines (1) challenges that federal entities face in their efforts to prevent prohibited items and individuals who may pose a security threat from entering GSA buildings and (2) actions that federal entities have taken to assess the effectiveness of their screening efforts and the results of those actions.

This report is a public version of a previously issued report identified by DHS and DOJ as containing information designated as For Official Use Only, which must be protected from public disclosure. Therefore, this report omits sensitive information regarding FPS's and USMS's covert- and intrusion-testing data, specific examples of the types of covert and intrusion tests these two entities used, and the names and locations of the buildings we visited, among other things. The information provided in this report is more limited in scope as it excludes such sensitive information, but it addresses the same questions as the For Official Use Only report and the overall methodology used for both reports is the same.

We selected two civilian federal tenant entities: the judiciary and the Social Security Administration (SSA). We selected the judiciary and SSA because the missions of these tenant entities result in high levels of public interaction and public visits to their offices within GSA buildings. We also selected the judiciary and SSA because they occupy a large proportion of GSA's federally owned building inventory, with the judiciary having the largest presence overall. We then identified a nongeneralizable sample of 11 federally owned buildings held by GSA with a facility security level (FSL) of IV, in three major metropolitan areas for our site visits. The Interagency Security Committee (ISC) defines the FSL categorization based on the analysis of several security-related

facility factors, which can range from security levels I to V, with a FSL V building considered to be the highest risk. The FSL serves as the basis for the implementation of physical security measures specified in ISC standards.[3] We selected these 11 buildings because FSL IV buildings are considered to have a "high" level of risk, and also based on a variety of other criteria, including the presence of our two selected tenant entities, recommendations received from agency officials, and, for FPS, possible inconsistencies in its data on prohibited items, among other factors.

To determine challenges federal entities face in their efforts to prevent prohibited items and individuals who may pose a security threat from entering GSA buildings, we interviewed GSA headquarters officials, FPS and USMS officials responsible for security issues at the headquarters level, FPS regional and USMS district level officials, and also officials at the building level for our 11 selected GSA buildings. Although information from our building visits is not generalizable to all GSA buildings, this information provides illustrative examples and context for our understanding of the challenges faced by FPS and USMS when conducting building security screening. This approach yielded diverse perspectives as our selected group of buildings varied in building type, use, size, and composition of federal tenant entities. We also reviewed FPS and USMS documentation on efforts to manage security screening, including security assessments and various reports for buildings we visited.

To determine actions federal entities have taken to assess the effectiveness of their screening efforts and the results of these efforts, we compared FPS's and USMS's efforts to comply with GAO's Standards for Internal Control in the Federal Government,[4] as well as to government-wide standards and key practices as identified by the ISC, including *The Risk Management Process for Federal Facilities* and the *Items Prohibited*

[3]A FSL V building is similar to a FSL IV building, but the building contains mission functions critical to national security such as the White House, the Pentagon, and the Central Intelligence Agency's headquarters building. FPS does not have security responsibility for FSL V buildings. ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013).

[4]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

from Federal Facilities.[5] We also reviewed FPS and USMS agency directives, policies, and guidance related to security-screening assessment tools. These FPS and USMS tools include conducting covert and intrusion tests and collecting data on prohibited items. In addition, we obtained and analyzed FPS and USMS data submissions for these assessment areas.[6] We also interviewed agency officials about data and conducted a data reliability assessment for the data we reviewed. We found the data on FPS covert tests and USMS intrusion tests were sufficiently reliable for describing the tests conducted from fiscal years 2010 through 2013 and the results of those tests. See appendix I for more details on our scope and methodology.

We conducted this performance audit from January 2014 to March 2015 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.

Background

GSA serves as federal agencies' landlord and designs, builds, manages, and maintains federal facilities. According to fiscal year 2013 data, over 8,900 buildings in the United States are held or leased by the GSA, and these buildings provide workspace for over 1-million federal employees and average 1.4-million daily visitors.[7] FPS, a subcomponent of the National Protection and Programs Directorate within DHS, is the primary agency responsible for providing law enforcement and related security services at GSA buildings.[8] USMS, a component of DOJ, has received

[5]ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013), and ISC, *Items Prohibited From Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: February 2013).

[6]Since FPS initiated its covert testing program in fiscal year 2010, we reviewed covert and intrusion testing data from FPS and USMS covering fiscal years 2010 through 2013. Additionally, we collected and analyzed 10 years of data on prohibited items from FPS and USMS, covering fiscal years 2004 through 2013.

[7]Of those buildings, almost 800 have a FSL of IV or V.

[8]To fund its operations, FPS charges fees for its security services to federal agencies in GSA-controlled facilities.

delegations of authority for building security from GSA and has primary responsibility for providing the security for federal judicial facilities and personnel.

Security screening consists of the electronic, visual, or manual inspection or search of persons, vehicles, packages, and containers for detecting the possession or attempted introduction of prohibited items including illegal and other dangerous items into a federal facility or secure area within a federal facility.[9] An individual in possession of or attempting to introduce a prohibited item, including an illegal or dangerous item into a federal building, is considered an individual who may pose a security threat. For the purposes of this report, we focused our efforts on the security screening of persons at access control points.[10] This process varies at each federal building based on a variety of factors, but a visitor to a FSL IV federal building, for example, may undergo a full security screening, which may include a protective security officer or court security officer checking his or her government-issued identification, having his or her belongings go through an x-ray machine, and the visitor physically walking through a walk-through magnetometer. Federal employees may undergo different levels of security screening at a federal building depending on a variety of security-related factors unique to that building. Screening of federal employees may range from a protective security officer or court security officer verifying that the employee has a valid government-issued identification card or an agency-issued credential, to full screening that would require the employee to go through a similar process as a visitor to a FSL IV federal building, as described above.

FPS's protective security officers—contract security guards—are the most visible component of FPS's operations, as well as the first contact with federal agencies for individuals entering a federal building. FPS relies heavily on its protective security officers and considers them to be the

[9]ISC, *Best Practices for Armed Security Officers in Federal Facilities*, 2nd ed. (Washington, D.C.: April 2013).

[10]Security screening access control points can include various areas of security screening such as building entrances, vehicle entrances, and mail processing. However, for the purposes of this report, we focused on security screening that occurs at building entrances, and in some cases, security screening areas within a building where a tenant agency requires additional screening prior to entering their designated office space. Throughout this report, we refer to these areas as security screening access control points.

entity's "eyes and ears" while performing their duties. FPS protective security officers are responsible for controlling access to federal buildings, conducting security screening at access control points, enforcing property rules and regulations, detecting and reporting criminal acts, and responding to emergency situations involving building safety and security. FPS protective security officers (1) control access to federal buildings by checking the identification of government employees who work there as well as members of the public who visit, and also (2) operate security-screening equipment, such as x-ray machines and walk-through magnetometers, to ensure prohibited items—including illegal items, such as firearms, explosives, knives, and drugs—do not enter federal buildings. In general, FPS protective security officers do not have arrest authority, but can detain individuals who are being disruptive or pose a danger to public safety.[11] According to FPS, it has around 13,000 protective security officers at approximately 2,700 of the 8,900 FPS-protected federal buildings across its 11 regions.[12] Of those, FPS conducts security screening of visitors and employees at approximately 2,400 buildings. FPS's budget for fiscal year 2014 was over $1.3 billion.

USMS has primary responsibility for protecting the federal judicial process by ensuring safe and secure conduct of proceedings and protecting federal judges, jurors, and members of the visiting public, in GSA buildings housing the judiciary. USMS's responsibilities include managing court security officers and security systems and equipment, including x-ray machines, surveillance cameras, duress alarms, and judicial chambers' entry control devices. USMS court security officers, also contract security guards, are responsible for screening for and intercepting weapons and other prohibited items from individuals attempting to bring them into federal courthouses. USMS court security officers also assist in providing security at facilities that house federal court operations. According to USMS, as of May 2014, USMS court security officers conducted entrance security screening at 410 federal buildings, 121 of which (approximately 30 percent) are multi-tenant

[11]Some FPS protective security officers may have arrest authority under conditions set forth by individual states.

[12]The protective security officers deployed by FPS to protect federal buildings are contract security guards procured through contracts with private security firms. FPS's area of responsibility covers the continental United States and U.S. territories. Headquartered in Washington, D.C., FPS is divided into 11 regions nationwide.

federal buildings across the 94 federal court districts.[13] USMS oversees the daily operation and management of security services performed by more than 5,000 court security officers.[14] The USMS's fiscal year 2014 enacted budget totaled more than $2.7 billion across multiple appropriations, with nearly $460 million designated for judicial and courthouse security.[15] The Judicial Conference of the United States is the principle policy-making body for administering the federal court system, and its Committee on Judicial Security recommends security policies for federal judges and courts. The Administrative Office of the United States Courts (AOUSC) coordinates with the federal courts, USMS, FPS, and GSA to implement the judiciary's security program.[16]

Since FPS is responsible for enforcing federal laws and regulations, and providing building entry and perimeter security at GSA buildings, among other responsibilities, FPS and USMS seek to closely coordinate security activities for federal buildings that contain courtrooms and judicial officers. The responsibilities for FPS and USMS are defined as part of a 1997 memorandum of agreement.

- More specifically, in multi-tenant federal buildings that are primarily courthouses (i.e., judicial or judicial-related space comprise more than 75 percent of the building), USMS provides court security officers for security screening at access control points at the building entrances,

[13]The court security officers deployed by the USMS to federal court facilities are contract security guards procured through contracts with private security firms. The geographical structure of the USMS mirrors the structure of United States district courts. There are 94 federal judicial districts, including at least one district in each state, the District of Columbia, the Commonwealths of Puerto Rico, and the Northern Mariana Islands and the two territories of the United States—the Virgin Islands and Guam.

[14]The court security-officer program is managed by the Judicial Security Division within USMS, and its Office of Court Security is responsible for managing and developing an effective nationwide physical security program for federal judiciary court facilities.

[15]USMS also designates funds for "Prisoner Security and Transportation," which is separate from "Judicial and Courthouse Security," but we did not include it in the $460-million figure since the focus of our report is on employee and public security-screening practices.

[16]USMS receives both direct appropriations and funding transferred from the judiciary for its courthouse security activities. Judicial Services has oversight for programs funded by the judiciary's court security appropriation. This funding provides for the court security-officer program, security equipment, and systems for space occupied by the judiciary.

access control, and security for all judicial areas while FPS may assist in providing perimeter-roving patrol and after hour coverage.

- In multi-tenant federal buildings that house federal courts, where judicial or judicial-related space comprise less than 75 percent of the building, FPS would generally provide protective security officers for security screening at access control points at the building entrances, as well as perimeter-roving patrol. USMS court security officers would conduct security screening at access control points for the judicial space within the building.

Currently, there are seven courthouses participating in a pilot program where USMS has also assumed control of perimeter security. The roles and responsibilities of USMS and FPS under this pilot program are outlined in a 2008 memorandum of understanding.

The ISC develops governmentwide physical security standards and best practices for federal security professionals responsible for protecting nonmilitary federal buildings in the United States. The ISC was established in 1995 by Executive Order 12977 following the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. The ISC is an interagency organization chaired by the DHS and is comprised of representatives from more than 50 federal agencies and departments. FPS is a member agency of the ISC, along with other federal entities such as GSA, USMS, SSA, and the federal judiciary. Executive Order 12977 directs each executive agency and department to cooperate and comply with the ISC policies and recommendations issued pursuant to the order.[17] The ISC's mission is to enhance the quality and effectiveness of the security and protection of nonmilitary federal buildings in the United States and to provide a permanent body to address continuing governmentwide security issues for these facilities. For example, in February 2013, the ISC developed a baseline list of items that are prohibited in federal buildings in order to provide some consistency.[18] Federal management regulations identify items generally

[17]Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 24, 1995), which established ISC, was subsequently amended by Executive Order 13286, Fed. Reg. 10619 (March 5, 2003). Executive agencies and departments are exempt from complying with ISC policies and recommendations if the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods.

[18]ISC, *Items Prohibited From Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: February 2013). The document also provides guidance on exemptions and exceptions on prohibited items in federal buildings.

prohibited from being introduced into a federal building—such as explosives, firearms, or other dangerous weapons—except for law enforcement purposes (and other limited circumstances).[19] The ISC standard also establishes a process for preventing prohibited items from entering into federal buildings and identifies responsibilities for denying entry to those individuals who attempt to enter with such items.

Federal buildings vary in their assigned FSL and implemented security countermeasures.[20] FPS is to coordinate with the building tenants, law enforcement and intelligence partners, and other stakeholders to gather information and identify the risks unique to each building being assessed. The initial evaluation of risks is used by FPS in calculating the FSL proposal. The facility security committee[21] or court security committee[22] then uses this proposal to establish the final FSL determination. FPS and USMS are to work in partnership with tenant facility security committees and court security committees to build a consensus regarding the type of countermeasures appropriate for each individual facility. Facility security committees and court security committees, which are composed of representatives of tenant entities at federal buildings and other stakeholders, have broad latitude in determining the security measures appropriate for their facility. The decision regarding the optimal combination of physical countermeasures (such as security barriers, x-ray machines, closed circuit television, and number and type of security-screening access control points staffed by FPS protective security officers and USMS court security officers) is based on a variety of factors. These

[19]41 C.F.R. §§ 102-74.435, 102-74.440.

[20]FPS defines a security countermeasure as a security device or procedure designed and implemented to mitigate the facility's risk to a specific credible threat.

[21]A facility security committee consists of representatives from each of the tenant entities in a federal facility. The facility security committee is responsible for addressing security issues at its respective facility and approving the implementation of security countermeasures.

[22]USMS is responsible for establishing a court security committee in each judicial district consisting of representatives from the USMS, clerk of the court, the U.S. Attorney, chief judge, FPS, and GSA, as appropriate. Depending on the district or individual courthouse, there can be a court security committee or a facility security committee, or both. In addition to these committees, coordination occurs at individual courthouses, as stakeholders implement their security roles and responsibilities.

factors include a facility security assessment report conducted by FPS,[23] the FSL, and the security needs of individual tenants. It is important to note that facility security committees and court security committees, rather than FPS and USMS, render the final decision regarding the number and type of security-screening access control points and technical countermeasures that are to be installed in each individual building. Facility security committees and court security committees have broad latitude in determining which items, if any, can be prohibited in their respective facilities, in addition to those specifically prohibited by law, as discussed later in the report.

FPS and USMS Face a Range of Challenges with Security Screening

FPS and USMS experience a range of challenges in their efforts to provide effective security screening. Such challenges can create a complex environment in which to conduct effective security screening. These challenges include: (1) building characteristics and location that may limit security options; (2) balancing security and public access; (3) operating with limited resources; (4) working with multiple federal tenants; and (5) effectively informing the public of prohibited items.

Building Characteristics and Location May Limit Security Options

Many GSA buildings were designed and constructed prior to the occurrence of several high-profile incidents where federal buildings were targets of acts of violence and consequently before security screening became more of a priority. GSA reported in 2011 that the lack of reinvestment funding is a challenge it faces as the average age of its buildings was 47 years old and has accelerated the deterioration of an already aged portfolio.[24] As a result, conducting security screening may be challenging for FPS and USMS because they have to work within the parameters of the building's original layout, physical location, and composition of tenants. For example, at the majority of the buildings that we visited, the public is required to undergo full screening upon entering the building, while employees typically undergo limited screening once their government identification cards are checked. However, according to USMS officials at a building that we visited, the layout of the building

[23]Facility security assessment reports are risk assessments that help FPS identify and evaluate potential risks so that countermeasures can be recommended to help prevent or mitigate risks.

[24]GSA Public Buildings Service, *State of the 2011 Portfolio* (Washington, D.C.: 2011).

makes it difficult for court security officers to conduct any type of security screening on the employees entering the building from the underground parking garage. The elevators to enter the building from the underground employee parking garage are physically located behind the building's screening access control points. As such, the employees who enter the building from the parking garage receive little to no screening beyond checking their identification cards upon entry into the garage. Further, according to USMS officials, in the instance that USMS determines the building needs to increase its security, it would be difficult to screen employees entering the building from the parking garage because the court security officers would not be able to utilize most of the screening equipment at the access control point due to the location of the elevators relative to the access control point.

Further, if a GSA building is considered to be historically significant—that is, it is listed on the National Register of Historic Places or is eligible for listing—renovations by federal agencies must follow the requirements of the National Historic Preservation Act of 1966, as amended.[25] Under the act, federal agencies are to use historic properties to the maximum extent feasible and retain and preserve the historic character of the property when making infrastructure changes or rehabilitating a property. As we have reported in the past, buildings listed on the National Register of Historic Places or aging buildings may not be able to support, or may make it more difficult to implement, security changes when complying with the National Historic Preservation Act's requirements.[26]

Also, when trying to make security screening enhancements that will alter the design or layout of a public space in a GSA building, such as to a security screening access control point for the public, FPS and USMS officials reported that it is challenging to coordinate such efforts with GSA due to factors including GSA's limited budget and initiatives such as GSA's First Impressions Program. The program emphasizes making better "first impressions" for the visiting public and also for the building's

[25]The National Historic Preservation Act of 1966 requires agencies to manage historic properties in keeping with their historic character, but it does not mandate a particular government decision; instead, it mandates a particular process for reaching a decision. See Pub. L. No. 89-665, 80 Stat. 915 (1966), codified as amended at 16 U.S.C. §§ 470-470x-6.

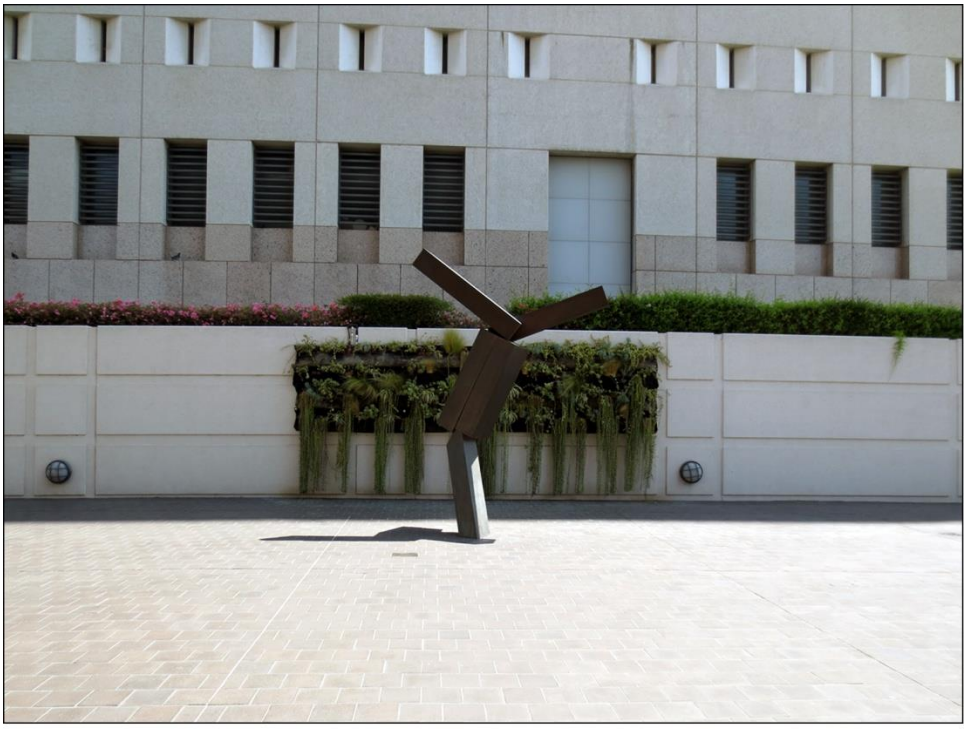
[26]GAO, *Federal Courthouses: Improved Collaboration Needed to Meet Demands of a Complex Security Environment,* GAO-11-857 (Washington, D.C.: Sept. 28, 2011).

tenants, in the public spaces of existing federal buildings. Therefore, GSA's First Impressions Program's goals can sometimes conflict with what the tenant entities or FPS or USMS believe to be needed screening-security enhancements. According to USMS officials, working with GSA can be challenging when trying to install new security enhancements or making alterations to the space because the changes may not meet the aesthetic framework GSA desired for the public space. For example, there is a severe glare caused by the sun's reflection through the windows into the lobby during a significant portion of the day, where the security screening access control point for the public is located at a building that we visited. According to USMS officials at the building, the glare obscures the court security officer's ability to see incoming visitors. The glare also affects the court security officer's view of the x-ray machine's computer monitor, potentially impeding the court security officer's ability to appropriately screen items sent through the x-ray machine (see fig. 1 below). However, according to USMS officials, GSA will not allow USMS to apply a tinting on the windows to reduce the impact of the glare because it would alter the aesthetics of the public space. At the time of our review, USMS and GSA had not resolved this issue. At a different entrance at the same building, solar glare made it difficult for court security officers to see individuals entering the building. USMS, however, was able to work with GSA to come up with a mutually agreeable solution. GSA suggested and created a "living wall" by planting foliage to help cover an exterior plain white wall, which had reflected sunlight into the building (see fig. 2 below).

Figure 1: Glare Affecting Screening of the Public at a Building We Visited

Source: GAO. | GAO-15-445

Figure 2: To Reduce Glare Affecting Screening, "Living Wall" Created Outside an Entrance at a Building We Visited



Source: GAO. | GAO-15-445

Balancing Security and Public Access

Striking an appropriate balance between providing security at federal buildings, and facilitating the public's access to government offices for services and other business transactions, continues to be a major challenge, as we have reported in the past. FPS and USMS officials at 6 of the 11 buildings we visited noted this challenge. We previously reported that GSA's goal is to create an environment that reflects an open, welcome atmosphere, as well as to protect against those with the intent to do harm. GSA also considers federal workers' convenience and privacy an important part of these considerations. For example, federal employees may undergo different levels of security screening depending on a variety of building-specific factors which may range from a federal identification check to a full screening, as the general public would experience. Federal agencies face particular challenges in GSA buildings with high public demand requiring regular public access. Such buildings include courthouses and federal office buildings that house agencies such

as the SSA, the United States Citizenship and Immigration Services (USCIS), and the Internal Revenue Service.[27]

According to the ISC, the potential threat to federal tenant entities within a multi-tenant building is based on several factors, which include, but are not limited to whether:

- the tenant entity's mission and interaction with certain segments of the public is adversarial in nature (e.g., criminal and bankruptcy courts, high-risk law enforcement);
- the tenant entity's mission draws attention of organized protest groups (e.g., Environmental Protection Agency, courthouses, Department of Energy); and
- the building is located in a high-crime area, as determined by local law enforcement.[28]

For example, according to SSA headquarters officials, the majority of challenges the agency experiences results from the tension between trying to provide effective security while accomplishing its mission. The SSA's mission is to deliver social security services that meet the needs of the public. To accomplish its mission, the SSA has 1,256 field offices where the agency provides in-person services to the public. Security has become such a pressing concern that there are armed FPS protective security officers at all SSA offices that involve customer interactions.[29] Furthermore, many field offices are specifically located in areas easily accessible to the public, which requires some offices to be located in higher risk crime areas, increasing their security risks.

In addition, a high volume of visitors to a federal building puts more pressure on the protective security officers and court security officers to effectively move visitors through the security screening process without compromising security standards. For example, at one building we visited, there is often a continuous line at the screening access control point at the public entrance and the building averages about 4,000 visitors

[27]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).

[28]ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013).

[29]In some instances, the SSA has delegated security authority from FPS, and would then be responsible for providing the armed security officers.

each day, primarily for services provided by USCIS or the Internal Revenue Service. USCIS created separate entrances with screening access control points at two buildings we visited, to provide additional security while also managing the number of visitors to the USCIS offices. At both buildings, USCIS paid for the dedicated screening access control points for its customers, including the screening equipment and the additional protective security officers. According to FPS officials at both buildings, USCIS funded the screening-security enhancements to better serve its customers and to streamline the process that would have been required had USCIS gone through the facility security committee's approval and budget process.

Operating with Limited Resources

According to FPS headquarters officials, some protective security officers are not fully trained to address all security-screening scenarios presented to them at screening-access control points. In 2010, 2013, and in 2014, we concluded that FPS continued to experience difficulty ensuring that its protective security officers have their required screening training and certifications, in part due to FPS's limited resources.[30] As a result, protective security officers deployed to federal buildings may have been operating x-ray and walk-through magnetometer equipment for which they have not been trained to use, thus raising questions about their ability to fulfill a primary responsibility at screening access control points.

We have made recommendations for FPS to improve upon its security-screening procedures, and FPS has taken some steps to do so.[31] Specifically, FPS has begun to implement its16-hour National Weapons Detection Training program. This program, referred to as "screener training," was included in all new solicitations for contract protective security-officer vendor companies issued in fiscal year 2014, according to

[30]GAO, *Federal Protective Service: Protecting Federal Facilities Remains a Challenge*, GAO-14-623T (Washington, D.C.: May 21, 2014); GAO, *Federal Protective Service: Challenges with Oversight of Contract Guard Program Still Exists, and Additional Management Controls Are Needed*, GAO-13-694 (Washington, D.C.: Sept. 17, 2013); and GAO, *Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards*, GAO-10-341 (Washington, D.C.: Apr. 13, 2010).

[31]GAO-14-623T; GAO-13-694; and GAO-10-341.

FPS headquarters officials.[32] This program doubles the screener training that protective security officers had received under prior contracts and includes performance-oriented training and testing. In February 2014, the first contract was awarded that included the 16-hour "screener training," according to FPS headquarters officials. FPS-certified inspectors are to provide the "screener training" to those protective security officers covered under the new contract. According to FPS officials at the headquarters and regional level, the initial feedback from the protective security officers who have undergone the new training has been very positive. The implementation of this program, however, will take time. Typically, protective security-officer vendor contracts are for 5-year periods, and according to a FPS headquarters official, contracts can be modified at any time to add within scope changes such as the new "screener training" provision. In addition, to offset resource demands on FPS for providing the additional "screener training" and to increase accountability for all new solicitations, FPS selected four contracts in three regions for a "Train the Trainer" pilot.[33] FPS is to train and certify instructors from the contract protective security officer companies at the National Weapons Detection Training program and the certified contract instructors are to then deliver the 16-hour training to their companies' respective contract protective security officers. FPS and the respective protective security officer companies modified four contracts in March 2014. The "Train the Trainer" pilot officially began in April 2014.[34]

Limited resources may contribute to the added challenge of not having enough protective security officers. According to FPS headquarters officials, limited staff is due to limited funding at the facility level (building-specific) or tenant agency level (tenant-specific). For example, despite

[32]According to FPS headquarters officials, the "screener training" measures the ability of a protective security officer to successfully complete a series of tasks, complete laboratory exercises, and pass an examination. Performance tasks include: properly operate the hand wand, find hidden items, and take appropriate action based on what officers find; properly operate the x-ray machine and correctly screen items presented, identify items in bags or packages, and take appropriate action based on what officers find; and properly operate the walk-through magnetometer and correctly identify personnel for secondary screening.

[33]The "Train the Trainer" pilot consists of two contracts from Region 11, one from Region 2, and one from Region 4.

[34]FPS is still in the process of considering expanding the "Train the Trainer" pilot program. FPS officials said they plan to run the pilot for one year and will subsequently make a decision as to whether to expand it to all contracts or certain contracts.

ISC standards that specify that each protective security officer should only be responsible for one screening task at a security-access control point, during our building visits, we found several instances when a protective security officer was conducting multiple screening tasks due to limited staff. For example, at one building we visited, there are three security screening access control points, each with two protective security officers who are responsible for (1) checking employee identification, (2) manning the x-ray machine, and (3) manning the walk-through magnetometer. According to an FPS regional official, despite the fact that this building is the largest building in the West Coast by square footage, there is a limited FPS presence on-site, relative to the size of the building. In some instances, a roving protective security officer may backfill at a security screening access control point if it gets busy, but screening may not be within his or her responsibilities or an area he or she is specifically trained in. At another building we visited, USMS officials made the decision to close one of its three security screening-access control points in November 2013 due to budget shortfalls.

According to USMS headquarters officials, obtaining adequate resources and funding is always an issue, but USMS is continuing to take steps to develop its security program. In 2013, USMS doubled the annual training requirement for court security officers, focused primarily on security screening. USMS is also examining the current level of court security officer training as compared with screening test passage rates, which we discuss below, to see if there are any trends and any potential actions that can be taken to improve its security training. Also, USMS headquarters officials told us that it would be helpful to have additional funding for more court security officers. As such, USMS is currently doing an analysis to determine the optimal number of court security officers that should be stationed at a security screening access control point, in order to determine the extent to which more resources may be needed in the field.

Working with Multiple Federal Tenants

Multi-tenant GSA buildings pose additional challenges in the security screening process because there are many federal stakeholders involved in the facility security committees and court security committees (if the judiciary is involved). As noted above, these stakeholders are responsible for building security screening decisions, among other security responsibilities. However, we found, as we did in August 2010, that tenant

entity representatives in the facility security committee may not have security knowledge or experience, but nonetheless are expected to make security decisions for their respective agencies.[35] During our site visits, multiple FPS regional and USMS district level officials identified the lack of security knowledge as a challenge in trying to work with federal tenants to implement recommended security-screening enhancements.

When FPS recommends countermeasures for a building in its facility security assessment, the facility security committee's chairperson[36] is made aware of the recommendations. For example, a recommended countermeasure may be to add an additional protective security officer, so each protective security officer is only responsible for one screening task at each screening access-control point, as outlined in ISC standards. FPS and USMS officials told us that federal tenant entities, who may have different needs, may not always agree with what level of security and security countermeasures are needed at their building, or agree with the costs that may be associated with those enhancements. Security countermeasures must compete with other program objectives for limited funding. Also, we previously found that the facility security committee's tenant-entity representatives often do not have the authority to commit their respective organizations to fund security countermeasures.[37] As a result, competing requirements, standards, and priorities for a building cannot always be reconciled, and the chairperson, on behalf of the facility or court security committee, may agree to accept the risk of not implementing a specific countermeasure. According to ISC policy, when a recommended countermeasure is not implemented, it must be clearly documented, as appropriate:

- Why the necessary level of protection cannot be achieved.
- What is the rationale for accepting the risk?
- What alternate strategies are being considered or implemented?
- What opportunities are in the future to implement the necessary level of protection?

[35]GAO, *Homeland Security: Addressing Weaknesses with Facility Security Committees Would Enhance Protection of Federal Facilities,* GAO-10-901 (Washington, D.C.: Aug. 5, 2010).

[36]Typically the facility security committee's chairperson is the senior representative of the tenant agency that occupies the largest area in the GSA building.

[37]GAO-10-901.

For example, some possible rationales for risk acceptance are: physical site or structural limitations, historical or architectural integrity, impact on an adjacent structure, and funding priorities.[38]

Executive branch agencies, with the exception of certain intelligence-related exemptions, are required to comply with the ISC's policies and recommendations. The ISC is required to develop a strategy for ensuring compliance with its standards; however, we previously found that the ISC did not formally monitor agencies' compliance with ISC standards, in part, because it lacks the staff and resources to conduct monitoring.[39] Currently, in place of a formal monitoring program, ISC officials hold quarterly meetings and participate in ISC's working groups along with their member agencies. ISC officials said that the information sharing that occurs through these channels helps them achieve a basic understanding of whether and how member agencies use the standards. This approach, however, does not provide a systematic assessment of ISC member agencies' use of the standards, and provides no information on non-member agencies' physical security practices. The ISC stated in its 2012 to 2017 action plan that it plans to establish protocols and processes for monitoring and testing compliance with its standards by fiscal year 2014.[40] We previously recommended that DHS direct ISC to conduct outreach to executive branch agencies to clarify how its standards are to be used, and develop and disseminate guidance on management practices for resource allocation as a supplement to the ISC's existing physical-security standards.[41] According to ISC officials, as of September 2014, the ISC has created a compliance working group and is in the beginning stages of developing a standard for ensuring compliance with its established policies.

[38]ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013).

[39]GAO, *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, GAO-14-86 (Washington, D.C.: Mar. 5, 2014).

[40]DHS, *Interagency Security Committee Action Plan 2012-2017.*

[41]GAO, *Facility Security: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies,* GAO-13-222 (Washington, D.C.: Jan. 24, 2013).

Effectively Informing the Public of Prohibited Items

FPS and USMS face challenges in effectively informing the visiting public about what items are prohibited from being brought into GSA buildings as lists of prohibited items vary among the buildings and among tenants in multi-tenant buildings. Based on various factors, such as the composition of federal tenants, and in the case of courthouses, decisions by judicial districts, each GSA building may have a unique list of prohibited items that, according to FPS and USMS officials, can cause some confusion to the visiting public. Facility security committees and court security committees have broad latitude in determining which items, in addition to those specifically prohibited by law (i.e., illegal items), can be prohibited from their facilities.[42] These additional items may not necessarily be "illegal." In addition, some items may be admissible for some individuals, while not for others. For example, a courthouse may restrict the general public from possessing a cell phone or laptop in a court space, but may permit such a device to be carried by a court employee or an attorney representing a client. Further, the visiting public may not know that an item is prohibited from the building until they are already there. In these instances, the protective security officer or court security officer might tell individuals to take the item back to their vehicle, or surrender the item. In some instances, court security officers may also be responsible for helping to store a prohibited item (such as a cell phone or laptop in a court space), until the individual returns to get it. According to USMS officials we met with, this adds to the responsibilities of the court security officers.

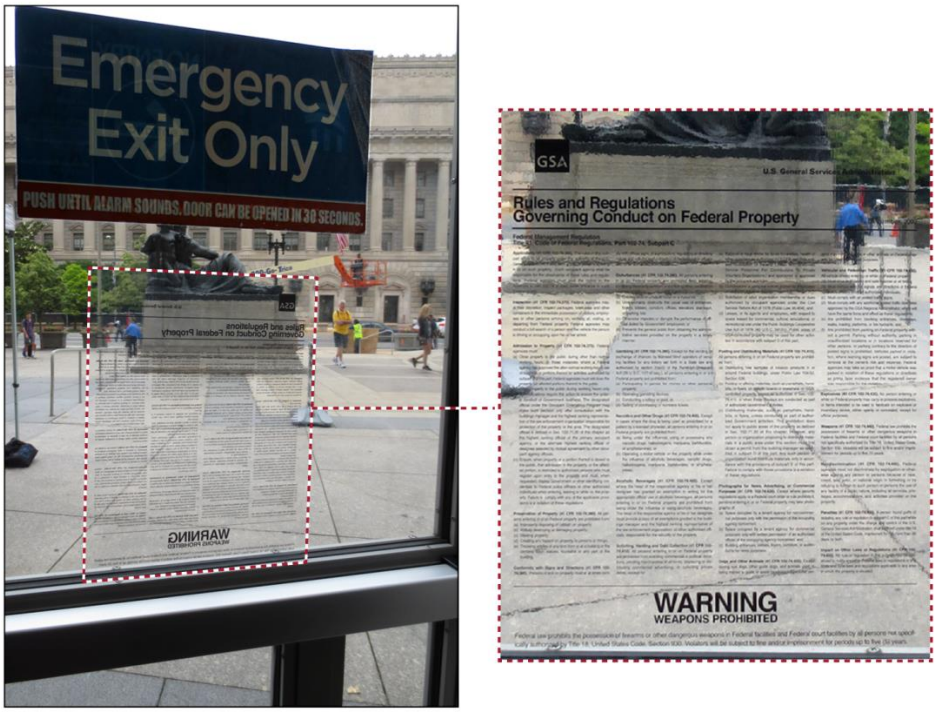
Though we did not specifically evaluate signage as part of this review, during our building visits, we observed a wide range in the types of signage posted informing the visiting public about what items were prohibited from the building. All signage in a GSA facility is under the direct control of the GSA building manager. GSA requires agencies to post signage at each of its buildings, such as signs that list prohibited items.[43] The facility security committee and court security committee work with the GSA building manager to ensure that signage is in place to inform their visitors and employees of the items that are prohibited within that building. However, we found that some signs were small, posted in

[42]Title 41 C.F.R. §§ 102-74.435, 102-74.440 identify and list items that are prohibited from being introduced into a federal facility except for law enforcement purposes and other limited circumstances. Those items are explosives, firearms, or other dangerous weapons.

[43]41 C.F.R. §§ 102-74.35, 102-74.385.

an obscure location, or very difficult to see or read (see fig. 3 below). We also saw some signs on the public entrance doors at one building we visited, with regulatory language on prohibited items from July 1999, even though current regulations were last revised in November 2005 (see fig. 4 below). Conversely, we found that some buildings had large, informative signs for visitors, and the signs were posted in key locations to help facilitate the security-screening process (see examples of signage in figs. 5 and 6 below).

Figure 3: An Example of a GSA Regulations Sign That Is Difficult to Read on a Door at a Building We Visited



Source: GAO. | GAO-15-445

Figure 4: Though Current Regulations Were Last Revised in November 2005, Dated Regulatory Language from July 1999 Found on the Public Entrance Doors at a Building We Visited

Source: GAO. | GAO-15-445

Figure 5: Signs Directing Visitors through the Security-Screening Process at a Building We Visited

Source: GAO. | GAO-15-445

Figure 6: Signs Directing Visitors through the Security-Screening Process at a Building We Visited

Source: GAO. | GAO-15-445

FPS and USMS Have Taken Steps to Assess Screening, but Each Lacks a Strategic Approach for Using the Data Collected to Improve Performance

Both FPS and USMS have taken steps to assess their security screening efforts such as conducting covert and intrusion tests and collecting data on prohibited items.[44] Our work showed that according to FPS data from fiscal years 2010 through 2013, FPS has experienced low covert-testing passage rates, and FPS has also limited the number of screening scenarios that can be used for testing. However, in fiscal years 2012 and 2013, for example, USMS data showed that court security officers passed 92 percent of intrusion tests on security screening. Although USMS tests more frequently than FPS, it has been unable to meet its intrusion-test frequency requirement per building each year. Also, FPS and USMS data on prohibited items show a wide variation in the number of items identified across buildings for both entities. Overall, FPS and USMS may use the results of covert and intrusion tests to address problems at the individual building or FPS region or USMS district level, to some degree, but they do not readily use the results to strategically assess performance nationwide. The benefits of using performance data in this strategic manner are reflected in ISC guidance, as well as key practices in security and internal control standards GAO has developed. Without a more strategic approach to assessing performance, both FPS and USMS are not well-positioned to improve security screening, identify trends and lessons learned, and address the aforementioned challenges related to screening in a complex security environment.

FPS and USMS Have Taken Steps to Assess Security-Screening Efforts

FPS and USMS have established testing programs to help officials assess security screening efforts at buildings they protect. For example, in 2010, FPS developed a policy requiring regional offices to conduct covert testing of security countermeasures with the goals of (1) assessing the effectiveness of countermeasures; (2) identifying policy and training deficiencies; (3) ensuring immediate corrective action; and (4) documenting, analyzing, and archiving results. As part of FPS's covert testing program, a "report of investigation" is to be developed after the conclusion of each test. In these reports, the responsible FPS official details the actions taken to prepare for each covert test, to execute it, and to assess it. USMS has also developed tools for measuring the effectiveness of its security screening practices at the building level. For example, USMS implemented a policy directive over 10 years ago for

[44]For the purposes of this report, we refer to unannounced testing of screening access control points as "covert tests" when conducted by FPS officials and "intrusion tests" for tests conducted by USMS officials.

conducting a specified number of intrusion tests on security-screening procedures at court facilities each year. These tests primarily consist of attempts to (1) circumvent the public-screening access control points of either the building or the judicial areas and (2) access the court building with a prohibited item such as a weapon. Following each intrusion test, USMS is to complete a facility-security test form that includes detailed information about the test conducted.

In addition to testing security-screening procedures, FPS and USMS also require protective security officers and court security officers to document prohibited items identified during the screening process. FPS policy requires protective security officers to document each prohibited item discovered by using a designated reporting form that includes information such as the item type and description. The data for each prohibited-item report are to be entered into FPS's web-based Enterprise Information System.[45] In USMS's statement of work for court security officers, these officers are responsible for providing statistical information on the number of prohibited items including weapons detected during the screening process, and USMS districts are responsible for reporting these items to the USMS Office of Court Security on a monthly basis. The data are compiled at the end of the fiscal year by the USMS Office of Court Security and forwarded to the AOUSC. According to USMS officials, this information is used for supporting, among other things, the AOUSC's annual budget request related to courthouse security.

Low FPS-Passage Rates on Covert Tests and Reduced Number of Testing Scenarios

FPS has consistently experienced low passage rates for covert tests since implementing its covert-testing program in fiscal year 2010. The covert-testing data we reviewed were from fiscal years 2010 through 2013 and related to buildings with a specific FSL. In addition, we found that in October 2012, FPS reduced the number of screening scenarios that can be used for covert testing. However, in December 2014, FPS reinstated some testing scenarios. For this publicly available report, we are not including the specifics about the covert tests themselves or the related passage rates due to the sensitivity of the information.

[45]The FPS policy applies to all facilities or properties under the control of the GSA and any facilities or properties owned, leased, or occupied by any federal agency contracting with FPS to provide security services. FPS Directive, 15.9.3.1, Prohibited Items Program (May 16, 2013). FPS's Enterprise Information System is a web-based program in which information is entered to report and record facility information.

USMS Court Security Officers Pass Most Intrusion Tests

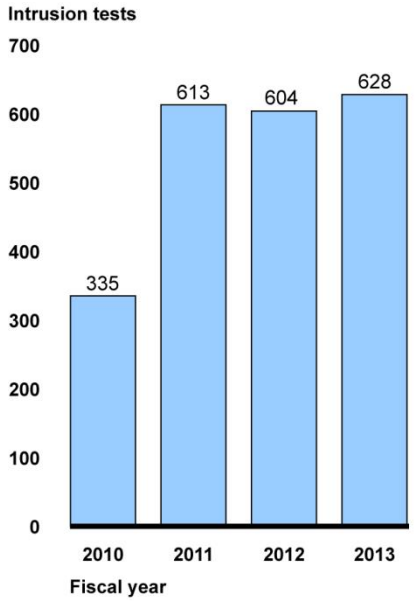
Since fiscal year 2010, USMS has recorded high-intrusion test passage rates, and USMS reported that it has experienced improvements in the effectiveness of its security-screening efforts for the years we reviewed.[46] For example, USMS reported that the intrusion-test passage rate for security-screening tests improved from 83 percent in fiscal year 2010, to 91 percent in fiscal year 2011, and to 92 percent in fiscal years 2012 and 2013.[47] Furthermore, USMS reported that it has improved its intrusion-test passage rate while consistently increasing the number of tests it conducted. For instance, in fiscal year 2010, USMS conducted 335 intrusion tests on security-screening procedures, and by fiscal year 2013, the agency nearly doubled that number by completing 628 intrusion tests on security-screening procedures.[48] See figure 7 for an overview of the number of USMS intrusion tests conducted from fiscal years 2010 through 2013 on security-screening procedures.

[46]For this report, we collected and analyzed USMS intrusion testing data from fiscal years 2010 through 2013.

[47]For the purposes of this report, we did not assess the comparability between FPS covert tests and USMS intrusion tests conducted. The passage rates reported are based on FPS and USMS data.

[48]In this section, we are only reporting on the USMS intrusion tests that targeted security-screening procedures.

Figure 7: Number of USMS Intrusion Tests on Security-Screening Procedures, Fiscal Years 2010–2013



Source: GAO analysis of USMS data. | GAO-15-445

USMS conducted significantly more intrusion tests than FPS conducted covert tests; however, we did not determine the reasons for this difference or what would constitute an adequate number of tests. Nevertheless, while USMS has increased the number of intrusion tests it conducts, we found that some USMS districts were conducting tests less frequently than required. Current USMS policy requires its 94 USMS districts to conduct an intrusion test at each court facility a specified number of times a year.[49] However, for the four USMS districts we visited, we found that none of the districts complied with this requirement. For example, one district we visited completed only 1 of the many intrusion tests it was required to conduct from fiscal years 2010 through 2013. Additionally, USMS conducts security screening at 11 buildings in another district we visited, and the district did not complete any covert tests during fiscal years 2012 and 2013. Furthermore, from fiscal years 2010 through 2013, USMS conducted only 14 percent of the intrusion tests that they

[49]In this section, we report on all USMS intrusion tests conducted from fiscal years 2010 through 2013, which include, but are not limited to, tests focused on security-screening procedures, as noted above.

were required to conduct at these 11 buildings. Overall, the 94 USMS districts conducted 45 percent of the total intrusion tests that USMS policy required these districts to conduct at their 410 buildings. Further, at the four USMS districts we visited, from fiscal years 2010 through 2013, there was a large range in each district's compliance rate from 2 percent to 63 percent. According to USMS headquarters officials, USMS lacks the appropriate resources to complete the required number of intrusion tests in each district. For example, USMS headquarters officials told us that each district manages its own resources and faces unique challenges that affect testing rates, such as the size of the district, geographical distances, workload, and manpower. As such, USMS is in the process of reviewing its current policy and expects to reduce the number intrusion tests required.

Data on Prohibited Items Show Wide Variations in the Number of Items Detected across Buildings

As discussed earlier, aside from their efforts to conduct covert and intrusion screening tests, FPS and USMS both collect data on prohibited items that are detected through the screening process. For example, FPS reported that in 2013, protective security officers detected approximately 700,000 prohibited items.[50] FPS policy directs FPS's Risk Management Branch to ensure that prohibited-items reports are collected correctly and that information is properly entered into the Enterprise Information System on a weekly basis.[51] However, our visits to selected FPS buildings and analysis of their reporting process indicated that these FPS data can vary widely from building to building.[52] For example, one building we visited reported over 230,000 prohibited items from fiscal years 2004 through 2013, an average of approximately 23,000 items per year. By contrast, a different building we visited reported just over 2,000 prohibited items during this same time period, an average of about 200 items per year, even though it is a much larger building with many more visitors (approximately 4,100 daily visitors) than the first building mentioned above (approximately 670 daily visitors).

[50]According to FPS policy, FPS protective security officers should direct the possessor to remove, from the facility, prohibited items that would otherwise be legal, and should take control of all illegal items detected during the screening process.

[51]FPS Directive, 15.9.3.1.

[52]For the purposes of this report, we collected and analyzed data on prohibited items provided by FPS and USMS from fiscal years 2004 through 2013.

Furthermore, for the larger building mentioned above, we identified 5 years (fiscal years 2009 through 2013) where no prohibited items were reported by FPS. However, during our visit to the building, FPS officials stated that prohibited items had been identified during that time period and provided physical evidence of prohibited items recently collected at the building (see fig. 8 below). According to FPS headquarters officials, in 2009, the prohibited items policy at the building—set by the facility security committee, not FPS—was for protective security officers to turn away anyone attempting to enter the building with a prohibited item. As a result, the protective security officers did not report identified prohibited items, believing that the policy was to report only items that had been confiscated. FPS headquarters officials stated that they had not been aware that there was a misinterpretation of the policy and that this resulted in a 5-year lapse in FPS oversight.

Figure 8: Prohibited Items Confiscated at a Building We Visited

Source: GAO. | GAO-15-445

We also reviewed data on prohibited items for FPS buildings that we did not visit and found that there were 295 buildings with no reported prohibited items during the 10-year period from fiscal years 2004 through 2013. These data alone would not allow us to definitively determine that prohibited items were detected and not reported at these buildings. However, the wide variation in the number of items detected warrants further analysis by FPS, which is discussed later in this report.

Similar to FPS, in assessing USMS's data on prohibited items, we found wide variations in the number of prohibited items identified during the security screening process. In fiscal year 2013, court security officers detected over 1.3 million prohibited items in federal courthouses, according to USMS data.[53] However, one USMS district we visited—District of Columbia—did not report detecting any prohibited items for 3 consecutive years (fiscal years 2005 through 2007) during the 10-year period we reviewed. In total, 24 of the 94 USMS districts (26 percent) did not report any prohibited items for at least 1 year, and 11 districts (12 percent) did not report prohibited items for multiple years during the 10-year period. According to USMS headquarters officials, in cases when no prohibited items are reported by a district, USMS headquarters officials accept that it is possible no prohibited items were identified or confiscated in a district, and no follow-up is conducted. As with FPS, however, the wide variation across buildings would warrant further analysis, which is discussed below.

Strategic Use of Performance Data Would Better Position FPS and USMS to Assess Screening Efforts

The benefits of using performance data strategically are reflected in ISC guidance, as well as key practices in security and internal control standards GAO has developed. The ISC identified the use of performance measurement and testing as a key management tool and reported that performance measurement data is essential to appropriate decision making on the allocation of resources.[54] In addition, our prior work on key practices in facility protection noted that monitoring and testing, as well as other methods of measuring performance, can help gauge the adequacy of facility protection, improve security, and ensure accountability for achieving goals.[55] We have also found that internal

[53]According to USMS policy, detected prohibited items shall be immediately brought to the visitor's attention, and are to be confiscated (e.g., illegal weapons) or given back to the individual for removal from the premises before entry is allowed.

[54]ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013).

[55]Our previous reports on key practices and performance measurement for facility protection discuss elements that contribute to effective measures of performance. See GAO, *Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts*, GAO-06-612 (Washington, D.C.: May 31, 2006) and 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).

control activities help ensure that management's directives are carried out and goals are met. Internal control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. These controls call for comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken.[56]

FPS officials said that they use covert testing to help determine weaknesses in personnel capabilities and performance at the building level. These weaknesses may then be addressed through training or corrective actions. The FPS officials also use covert testing to determine gaps in screening, security countermeasures, and access control processes at the building level. However, FPS headquarters officials also said that that they had difficulty determining how to use the test results for improving their security-screening efforts overall. For example, they said there are multiple reasons why a protective security officer or screening access control point can fail a covert test such as: poor protective-security-officer performance (e.g., a protective security officer may have ignored training or access control point instructions); insufficient training; and security-screening systems or conditions that may not be conducive to success (e.g., inadequate lighting or unsuitable position of screening equipment). FPS's difficulty in using the covert test results may stem from its lack of a strategy or systematic approach to linking performance data with corrective actions on a nationwide basis by determining trends and helping inform which types of scenarios to use for the covert tests. Even though FPS collects covert-testing data, it does not systematically analyze the data at the headquarters or regional level. A systematic analysis of data could help FPS adhere to the internal control standard related to data analyses and comparisons, and be better-positioned to target the primary causes for covert test failures.

While USMS has experienced higher intrusion-test passage rates, it similarly lacks a strategic approach to using and analyzing screening data that could aid in further improving its passage rates. USMS headquarters officials said that they do not systematically analyze intrusion-testing data. Instead, they collect testing data to measure the quality of services that

[56]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

contractors provide at the district level, and they feel that their current reporting efforts accomplish that goal. USMS headquarters also does not conduct any follow-up with its districts to ensure compliance with the intrusion-testing program, and testing data are not used to comprehensively assess the program. Nonetheless, these data could be useful to USMS in determining whether its intrusion-test passage rates are acceptable and whether goals should be set for higher passage rates. Greater use of the data could also help USMS determine the number and frequency of tests that would be adequate and attainable within its available resources.

A more strategic approach to assessing screening efforts could also include analyses of data on prohibited items. FPS and USMS do not conduct systematic analyses of the data on prohibited items they collect. At the time of our review, FPS officials told us that they did not conduct any follow up with the regions that did not report on the prohibited items they identified. USMS headquarters officials said that prohibited items are defined by individual districts, which makes data across districts difficult to compare. However, a more strategic approach to analyzing data on prohibited items would allow FPS and USMS to determine (1) the reasons for wide variations in these data, (2) whether data are incomplete, and (3) if there are lessons learned that could be applied nationwide. It may also be useful in determining how best to communicate prohibited items policy to the public through signage.

Conclusions

Federal buildings held and leased by GSA have been targets of acts of violence in recent years and providing security screening at these buildings can be challenging for a variety of reasons, including balancing security and public access and operating with limited resources. Due to the sensitivity of certain FPS and USMS information regarding covert and intrusion testing, that information was omitted for the purposes of this publicly available report. However, the results of our analysis of all the information we reviewed provided the groundwork for our recommendations to both DHS and DOJ—actions we believe will improve FPS's and USMS's security-screening efforts. In recent years, FPS and USMS have taken steps to improve their security-screening efforts, such as implementing various policies, conducting covert and intrusion tests of security-screening procedures, and collecting data on prohibited items identified at screening access control points. However, FPS has experienced low covert-testing passage rates and has limited the number of security-screening testing scenarios it uses during covert tests. USMS has recorded higher intrusion-test passage rates. And although USMS

tests security screening more frequently than FPS, it has been unable to meet its intrusion-test-frequency requirement. Also, FPS and USMS data on prohibited items show wide variation in the number of items identified across buildings. Compounding these issues, both entities lack an approach or strategy to systemically assess screening performance. The benefits of using performance data in this manner are reflected in ISC guidance, as well as key practices in security and internal control standards that GAO has developed. Without a more strategic approach to assessing performance, FPS and USMS are not well-positioned to improve security screening, to identify trends and lessons learned, and to address the range of challenges related to screening in a complex security environment.

Recommendations for Executive Action

We are making two recommendations—one to the Secretary of the Department of Homeland Security and one to the Attorney General:

We recommend that the Secretary of the Department of Homeland Security direct FPS to develop and implement a strategy for using covert-testing data and data on prohibited items to improve FPS's security-screening efforts. The strategy should, at a minimum, aim to ensure that:

- covert-testing data are used to systematically monitor, review, and improve performance nationwide;
- covert-testing data are used to determine which testing scenarios will be implemented or reinstated; and
- data on prohibited items are analyzed to determine the reasons for wide variations in the number of reported prohibited-items detected across buildings and to assist with managing the screening process and informing policy.

We recommend that the Attorney General direct USMS to develop and implement a strategy for using intrusion-testing data and data on prohibited items to improve USMS's security-screening efforts at federal courthouses held by GSA. The strategy should, at a minimum, aim to ensure that:

- intrusion-testing data is used to systematically monitor and review performance nationwide;
- intrusion-testing data are used to determine, with stakeholders, what frequency of testing is appropriate; and
- data on prohibited items are analyzed to determine the reasons for wide variations in the number of reported prohibited-items detected

across buildings and to assist with managing the screening process and informing policy.

Agency Comments

We provided a draft of this report to the AOUSC, DHS, DOJ, GSA, and SSA for review and comment. DHS and DOJ concurred with the recommendations directed at FPS and USMS, respectively. DHS stated that moving forward, FPS will continue to develop an overall strategy to better define how to leverage covert testing and prohibited items data to systematically monitor, analyze, and improve screening processes nationwide and inform policy. DHS's official written response is reprinted in appendix II. DOJ conveyed its concurrence with the recommendation in an e-mail. AOUSC, DHS, DOJ, and GSA provided technical comments, which we incorporated as appropriate. SSA agreed with the report as written and did not have any technical comments.

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 to the appropriate congressional committees; the Director of AOUSC; the Secretary of Homeland Security; the Attorney General of the United States; the Administrator of GSA; and the Commissioner of SSA. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff 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 key contributions to this report are listed in appendix III.

Sincerely yours,

Mark L. Goldstein
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

This report focuses on security screening at General Services Administration (GSA) buildings. Specifically, our review addressed the following questions: (1) What challenges do federal entities face in their efforts to prevent prohibited items and individuals who may pose a security threat from entering GSA buildings? and (2) What actions have these federal entities taken to assess the effectiveness of their screening efforts, and what have been the results?

This report is a public version of a previously issued report identified by DHS and DOJ as containing information designated as For Official Use Only, which must be protected from public disclosure. Therefore, this report omits sensitive information regarding FPS's and USMS's covert- and intrusion-testing data, specific examples of the types of covert and intrusion tests these two entities used, and the names and locations of the buildings we visited, among other things. The information provided in this report is more limited in scope as it excludes such sensitive information, but it addresses the same questions as the For Official Use Only report and the overall methodology used for both reports is the same.

For our review, we selected two civilian federal tenant entities: the judiciary and the Social Security Administration (SSA).[1] We selected the judiciary and SSA because the missions of these tenant entities result in high levels of public interaction and public visits to their offices within GSA buildings. We also selected the judiciary and SSA because they occupy a large proportion of GSA's federally owned building inventory, with the judiciary having the largest presence overall. For the purposes of this report, we focused our efforts on the security screening of persons.

To inform both objectives, we selected a nongeneralizable sample of 11 federally owned buildings held by GSA in three major metropolitan areas for our site visits. The focus of our review was on federally owned buildings held by GSA with a facility security level (FSL) IV.[2] We selected

[1]For the purposes of this report, we limited our review to civilian federal agencies and did not include the Department of Defense.

[2]The Interagency Security Committee (ISC) defines the FSL categorization based on the analysis of several security-related facility factors, which can range from security levels I to V. The FSL serves as the basis for the implementation of physical security measures specified in ISC standards. ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013).

these 11 buildings because FSL IV buildings are considered to have a "high" level of risk, and also based on a variety of other criteria, including the presence of our two selected tenant entities, recommendations received from agency officials, and, for the Federal Protective Service (FPS), possible inconsistencies in its data on prohibited items.

To determine challenges federal entities face in their efforts to prevent prohibited items and individuals who may pose a security threat from entering GSA buildings, we interviewed GSA headquarters officials, FPS and USMS officials responsible for security issues at the headquarters level, FPS regional and USMS district level officials, and also officials at the building level for our 11 selected GSA buildings. FPS is the primary agency responsible for providing law enforcement and related security services at GSA buildings. USMS has primary responsibility for various aspects of protecting federal courthouses and other federal buildings with a court presence. Although information from our building visits is not generalizable to all GSA buildings, this information provides illustrative examples and context to our understanding of the challenges faced by FPS and USMS when conducting building security screening. This approach yielded diverse perspectives as our selected group of buildings varied in building type, use, size, and composition of federal tenant entities. Prior to our building visits, we reviewed FPS and USMS documentation on efforts to manage security screening. We requested and reviewed security assessments and reports for buildings we visited as well as other buildings located in the FPS regions and USMS districts we visited, to the extent they were available. In preparation for our site visits, we also provided the appropriate FPS regional and USMS district officials with a series of questions regarding security-screening challenges, and asked for their responses. To further understand the challenges that FPS and USMS may face, we also spoke with members of the National Association of Security Companies, which is the nation's largest contract security officer association and its membership includes companies that provide government contract security officers. The National Association of Security Companies officials provided their perspectives regarding security screening issues at federal buildings, such as challenges faced by security officers.

To determine actions federal entities have taken to assess the effectiveness of their screening efforts and the results of these efforts, we compared FPS's and USMS's efforts to comply with the Interagency

Security Committee's (ISC) standards, including *The Risk Management Process for Federal Facilities* and the *Items Prohibited from Federal Facilities*.[3] We also reviewed FPS and USMS agency directives, policies, and guidance related to assessment tools such as collecting data on prohibited items and conducting covert and intrusion tests at security-screening entrances, and we obtained and analyzed FPS and USMS data submissions for these assessment areas. For example, we reviewed FPS and USMS's data on prohibited items from fiscal years 2004 through 2013. For FPS, we also obtained covert-testing data at the national, regional, and building level from fiscal years 2010 through 2013. For USMS, we obtained agency-wide results of its intrusion tests and detailed data for the districts we visited from fiscal years 2010 through 2013.[4] To gather detailed examples of security-screening data issues and to learn about the processes by which data are collected and submitted, we compared our findings from our building visits with the data provided by selected agencies. We then assessed FPS's and USMS's processes for managing these data against agency requirements and GAO's Standards for Internal Control in the Federal Government.[5] According to GAO's standards for internal control, internal controls are a major part of managing an organization and comprise the plans, methods, and procedures used to meet missions, goals, and objectives. Internal controls, which are synonymous with management controls, help government program managers achieve desired results through effective stewardship of public resources, and control activities contribute to data's

[3]The ISC is an interagency organization chaired by the DHS, comprised of representatives from more than 50 federal agencies and departments, and it establishes standards and best practices for federal security professionals responsible for protecting non-military federal facilities in the United States. FPS is a member agency of the ISC, along with other federal agencies such as GSA, USMS, SSA, and the federal judiciary. ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: August 2013) and ISC, *Items Prohibited From Federal Facilities: An Interagency Security Committee Standard* (Washington, D.C.: February 2013).

[4]USMS does not collect and track intrusion testing data by districts and buildings. Instead, USMS develops a description of intrusion-testing results combined for all districts, by fiscal year.

[5]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

accuracy and completeness.[6] We also interviewed agency officials about the data and conducted a data reliability assessment for the data we reviewed. We posed questions to officials at FPS and USMS about the collection and reporting of prohibited items and covert and intrusion-testing data. We determined that the agencies' data on prohibited items are not always complete or properly reported. As a result, agencies cannot ensure that prohibited-items data are sufficiently reliable to support sound management and decision making about security-screening issues. However, based on information gathered for covert and intrusion tests conducted by FPS and USMS, we determined that the data were sufficiently reliable for describing the tests conducted from fiscal years 2010 through 2013 and the results of those tests.

We conducted this performance audit from January 2014 to March 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[6]Control activities can include activities such as reconciliations performed to verify data completeness; an agency's data-entry design features to improve data accuracy; data validation and editing performed to identify erroneous data; and erroneous data that is captured, reported, investigated, and promptly corrected.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

March 11, 2015

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

Re: Draft Report GAO-15-445, "HOMELAND SECURITY: Actions Needed to Better Manage Security Screening at Federal Buildings and Courthouses"

Dear Mr. Goldstein:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's (1) acknowledgment of the range of challenges DHS's National Protection and Programs Directorate Federal Protective Service (FPS) experiences in its effort to provide effective security screening, and (2) recognition of efforts FPS has taken to enhance its presence and security at various federal buildings it protects in light of recent world events targeting government personnel and buildings. This includes actions taken by FPS to enhance security screening efforts such as conducting covert and intrusion tests and collecting prohibited-item data.

The draft report contained one recommendation for DHS with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct FPS to:

Recommendation: Develop and implement a strategy for using covert testing and prohibited item performance data to improve its security screening efforts. The strategy should, at a minimum, aim to ensure that:

- Covert testing data are used to systematically monitor, review and improve performance nationwide;

- Covert testing data are used to determine which testing scenarios will be implemented or reinstated; and,
- Prohibited items data are analyzed to determine the reasons for wide variations in the number of reported prohibited items detected across buildings, and to assist with managing the screening process and informing policy.

Response: Concur. Data resulting from covert security testing and prohibited items screening is something that FPS can better utilize to test the effectiveness of countermeasures and make recommendations for the improvement of security procedures, training, and technology. The FPS Training and Professional Development Division has already initiated efforts to develop and implement measures for using this data to improve its security screening efforts. For example, FPS identified the need for additional Protective Security Officer (PSO) training, and, after further evaluation of the program, an enhanced training emphasis has been instituted for the PSOs. In addition, FPS recently decided to reinstate several covert test scenarios with the goal of incrementally resuming full testing.

Moving forward, FPS will continue to develop an overall strategy to better define how to leverage covert testing and prohibited items data to systematically monitor, analyze and improve screening processes nationwide and inform policy. The strategy will also address covert testing scenarios and provide a process through which they are selected, implemented, and evaluated in conjunction with the performance data. Estimated Completion Date: December 31, 2015.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

2

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, other key contributors to this report were David Sausville, Assistant Director; Catherine Kim, Analyst-in Charge; Russell Burnett; Raymond Griffith; Geoffrey Hamilton; Delwen Jones; Hannah Laufe; Tom Lombardi; and Josh Ormond.