United States Government Accountability Office

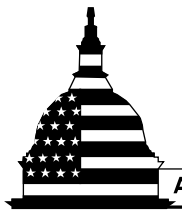
GAO

Report to the Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

August 2012

FEDERAL PROTECTIVE SERVICE

Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities



G A O

Accountability * Integrity * Reliability

GAO-12-739

August 2012

FEDERAL PROTECTIVE SERVICE

Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-739, a report to the Chairman of the Subcommitee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

FPS provides security and law enforcement services to over 9,000 federal facilities under the custody and control of the General Services Administration (GSA). GAO has reported that FPS faces challenges providing security services, particularly completing FSAs and managing its contract guard program. To address these challenges, FPS spent about $35 million and 4 years developing RAMP—essentially a risk assessment and contract guard oversight tool. However, RAMP ultimately could not be used because of system problems.

GAO was asked to examine (1) the extent to which FPS is completing risk assessments; (2) the status of FPS's efforts to develop an FSA tool; and (3) FPS's efforts to manage its contract guard workforce. GAO reviewed FPS documents, conducted site visits at 3 of FPS's 11 regions, and interviewed FPS officials and inspectors, guard companies, and 4 risk management experts.

What GAO Recommends

GAO recommends that FPS incorporate *NIPP*'s risk management framework in any future risk assessment tool; coordinate with federal agencies to reduce any unnecessary duplication in FPS's assessments; address limitations with its interim tool to better assess federal facilities; develop and implement a comprehensive and reliable contract guard oversight system; and independently verify that its contract guards are current on all training and certification requirements. DHS concurred with GAO's recommendations.

View GAO-12-739. 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) is not assessing risks at federal facilities in a manner consistent with standards such as the *National Infrastructure Protection Plan's* (*NIPP*) risk management framework, as FPS originally planned. Instead of conducting risk assessments, since September 2011, FPS's inspectors have collected information, such as the location, purpose, agency contacts, and current countermeasures (e.g., perimeter security, access controls, and closed-circuit television systems). This information notwithstanding, FPS has a backlog of federal facilities that have not been assessed for several years. According to FPS's data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012. However, GAO was unable to determine the extent of FPS's facility security assessment (FSA) backlog because the data were unreliable. Multiple agencies have expended resources to conduct risk assessments, even though the agencies also already pay FPS for this service. FPS received $236 million in basic security fees from agencies to conduct FSAs and other security services in fiscal year 2011. Beyond not having a reliable tool for conducting assessments, FPS continues to lack reliable data, which has hampered the agency's ability to manage its FSA program.

FPS has an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool (MIST), which it plans to use to assess federal facilities until it develops a longer-term solution. According to FPS, once implemented, MIST will allow it to resume assessing federal facilities' vulnerabilities and recommend countermeasures—something FPS has not done consistently for several years. Furthermore, in developing MIST, FPS generally followed GAO's project management best practices, such as conducting user acceptance testing. However, MIST has some limitations. Most notably, MIST does not estimate the consequences of an undesirable event occurring at a facility. Three of the four risk assessment experts GAO spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess risks. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design and thus requires more time to validate. MIST also was not designed to compare risks across federal facilities. Thus, FPS has limited assurance that critical risks at federal facilities are being prioritized and mitigated.

FPS continues to face challenges in overseeing its approximately 12,500 contract guards. FPS developed the Risk Assessment and Management Program (RAMP) to help it oversee its contract guard workforce by (1) verifying that guards are trained and certified, and (2) conducting guard post inspections. However, FPS faced challenges using RAMP, such as verifying guard training and certification information, for either purpose and has recently determined that it would no longer use RAMP. Without a comprehensive system, it is more difficult for FPS to oversee its contract guard workforce. FPS is verifying guard certification and training information by conducting monthly audits of guard contractor training and certification information. However, FPS does not independently verify the contractor's information. Additionally, according to FPS officials, FPS recently decided to deploy a new interim method to record post inspections to replace RAMP.

Contents

Abbreviations

DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
FSA	facility security assessment
FSC	Facility Security Committee
FSL	facility security level
FSRM	Federal Security Risk Manager
GSA	General Services Administration
IG	Inspector General
IP	Office of Infrastructure Protection
IRS	Internal Revenue Service
IRVS	Integrated Rapid Visual Screening of Buildings
ISC	Interagency Security Committee
IST	Infrastructure Survey Tool
MIST	Modified Infrastructure Survey Tool
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
RAMP	Risk Assessment and Management Program
S&T	Science and Technology Directorate

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 10, 2012

The Honorable Daniel E. Lungren
Chairman
Subcommittee on Cybersecurity, Infrastructure Protection,
and Security Technologies, Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

Federal facilities are among the targets for terrorist attacks and other acts of violence, as evidenced by the 2012 shooting at the Anderson Federal Building in Long Beach, California, and the 2011 attempted bombing of the McNamara Federal Building in Detroit, Michigan. These incidents highlight the importance of protecting the over one million government employees who work in, as well as the public who visit, the more than 9,000 federal facilities under the custody and control of the General Services Administration (GSA). As a component of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), the Federal Protective Service (FPS) is the primary agency responsible for protecting these facilities. FPS provides physical security services, such as conducting risk assessments, which FPS refers to as facility security assessments (FSA), and responds to incidents at federal facilities. An FSA helps FPS identify and evaluate potential risks so that countermeasures can be recommended to help prevent or mitigate these risks.

We have previously reported that FPS faces long-standing challenges in providing security services, particularly in completing quality risk assessments in a timely manner and overseeing its contract guard program. To address challenges related to FPS's FSA process and contract guard oversight, FPS developed the Risk Assessment and Management Program (RAMP), a Web-enabled FSA and guard management system, which was implemented in November 2009. We reported in July 2011 that FPS spent about $35 million and took almost 4 years developing RAMP—$14 million and 2 years more than planned.[1]

[1]GAO, *Federal Protective Service: Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS's Risk Assessment and Management Program*, GAO-11-705R (Washington, D.C.: July 15, 2011).

However, RAMP could not be used to complete FSAs because of several factors, including that FPS did not verify the accuracy of federal facility data used. As a result, FPS's Director decided that the agency would stop using RAMP to conduct FSAs and instead pursue an interim tool to replace it. In September 2011, FPS began working with Argonne National Laboratory to develop a vulnerability assessment tool referred to as the Modified Infrastructure Survey Tool (MIST). FPS plans to use MIST to assess the vulnerabilities of federal facilities until the agency develops a permanent replacement for RAMP. FPS also developed RAMP to (1) provide accurate and reliable records of its contract guards' training and certifications that FPS could use to verify that guards deployed at federal facilities are qualified and (2) to conduct guard post inspections. In July 2011, we reported that FPS had experienced difficulty using RAMP to ensure that its guards met training and certification requirements, primarily because of challenges with verifying RAMP's guard data.[2] FPS concurred with our recommendation to determine whether it was cost beneficial to continue to use RAMP for guard oversight. On June 15, 2012, FPS decided to no longer use RAMP to help oversee its contract guard program.

Given FPS's challenges, you requested that we examine FPS's current efforts to conduct FSAs and oversee its contract guard workforce. This report examines the extent to which FPS is (1) completing risk assessments, (2) developing a tool to complete FSAs, and (3) managing its contract guard workforce. To examine the extent to which FPS is completing risk assessments and overseeing guards without RAMP, we reviewed, among other things, FPS's current FSA procedures and data on completed and planned FSAs for fiscal years 2010 to 2012. Specifically, we reviewed FPS's FSA data aggregated from its 11 regions to determine the extent of its FSA backlog. However, we could not determine the extent of the backlog because FPS's data contained a number of missing and incorrect values that made it unreliable. We also visited 3 of FPS's 11 regions and interviewed internal and external stakeholders including, among others, FPS, GSA, Department of Veterans Affairs, the Federal Highway Administration, Immigration and Customs Enforcement, and guard companies. We selected these 3 regions based on the number of federal facilities in the region and their security levels, the number of contract guards in the region, and

[2]GAO-11-705R.

geographic dispersion. Our work is not generalizable to all FPS regions. To determine the status of FPS's efforts to develop an FSA tool, we reviewed, among other things, relevant project documents for MIST and federal physical security standards, such as DHS's *National Infrastructure Protection Plan's* (*NIPP*) risk management framework. We also interviewed FPS officials, representatives from Argonne National Laboratory who are responsible for developing MIST, and four risk management experts. We selected our four risk assessment experts from a list of individuals who participated in the Comptroller General's 2007 risk management forum.[3]

We conducted this performance audit from July 2011 through August 2012 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. See appendix I for more detailed information on our scope and methodology.

Background

To achieve its facility protection mission, in fiscal year 2012, FPS has a budget of $1.3 billion; over 1,200 full-time employees; and about 12,500 contract security guards. Contract guards are responsible for controlling access to federal facilities, screening access areas to prevent the introduction of weapons and explosives, enforcing property rules and regulations, detecting and reporting criminal acts, and responding to emergency situations involving facility safety and security. FPS relies on the fees it is authorized to charge federal tenant agencies in GSA-controlled facilities for its security services to fund its operations.[4] For example, FPS charges tenant agencies a basic security fee (currently $0.74 cents per square foot) to, among other things, conduct FSAs, monitor alarms and dispatch operations, and perform law enforcement activities.

[3]GAO, *Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-627SP (Washington, D.C.: April 2008).

[4]40 U.S.C. 586; 41 C.F.R. § 102-85.35; Pub. L. No. 111-83, 123 Stat. 2142, 2156-57 (2009).

FPS's FSA process generally entails:

- gathering and reviewing facility information;
- conducting and recording interviews with tenant agencies;
- assessing threats, vulnerabilities, and consequences to facilities, employees, and the public; and
- recommending countermeasures to federal tenant agencies.

To carry out this process, FPS's long-term goal has been to develop a tool that aligns with DHS's *NIPP* risk-management framework and Interagency Security Committee (ISC) standards.[5] According to the *NIPP*, a risk assessment should assess threats, vulnerabilities, consequences, and recommend countermeasures, specifically:

- A *threat* assessment is the identification and evaluation of adverse events that can harm or damage an asset.
- A *vulnerability* assessment identifies weaknesses in physical structures, personal protection systems, processes, or other areas that may be exploited.
- A *consequence* assessment is the process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence.

After these three assessments are completed, the information is used to determine whether a facility's risk is low, medium, or high. Additionally, the *NIPP* and ISC state that an agency's risk assessment methodology should be

- credible (or complete) as able to assess the threat, vulnerability, and consequences of specific acts;
- reproducible as able to produce similar or identical results when applied by various security professionals; and
- defensible as able to provide sufficient justification for deviations from the ISC defined security baseline.

[5]The ISC is comprised of representatives from more than 50 federal agencies and departments, establishes standards and best practices for federal security professionals responsible for protecting non-military federal facilities in the U.S. FPS is a member agency of the Interagency Security Committee in the Department of Homeland Security, along with other federal agencies such as the General Services Administration, the Federal Aviation Administration, the Environmental Protection Agency, and other components within the Department of Homeland Security.

In addition, as part of its FSA process, FPS also uses the ISC's *Facility Security Level Determination for Federal Facilities* to determine the facility security level (FSL). The ISC recommends that level I and II facilities be assessed every 5 years and level III and IV facilities every 3 years, and according to the ISC's criteria:

- A level I facility may be 10,000 or fewer square feet, have fewer than 100 employees, provide administrative or direct service activities, and have little to no public contact.
- A level II facility may be 100,000 or fewer square feet, have 250 or fewer employees, be readily identifiable as a federal facility, and provide district or statewide services.
- A level III facility may be 250,000 or fewer square feet, have 750 or fewer employees, be an agency's headquarters, and be located in an area of moderate crime.
- A level IV facility may exceed 250,000 square feet, have more than 750 employees, house national leadership, and be located in or near a popular tourist destination.

Since 2000, FPS has used three different tools to assess federal facilities and the assessment has varied, as shown in table 1.

Table 1: FPS's Past FSA Tools

Tools	Time frame used	Description
Federal Security Risk Manager (FSRM)	2000 to November 2009	FSRM was a stand-alone computer assessment tool. With this tool, FPS's inspectors used a subjective approach to completing assessments and recommending countermeasures. However, FSRM did not assess risk according to the *NIPP's* risk management framework methodology or allow comprehensive analysis as the reports were not entered into a database.
Risk Assessment and Management Program (RAMP)	November 2009 to June 2010	RAMP was a Web-based risk assessment and guard management tool. It was designed to calculate risks based on threat, vulnerability, and consequence using *NIPP's* risk management framework methodology. However, RAMP did not incorporate ISC's *Physical Security Criteria for Federal Facilities* because they were not finalized until after RAMP was developed.
FSA Calculator and Template	July 2010 to June 2011	The FSA calculator and template was an Excel spreadsheet and Word document that FPS's inspectors used to assess a facility's threat, vulnerability and consequence. After the assessments were completed, FPS planned to provide tenant agencies with a report with recommended countermeasures. The FSA calculator included RAMP's risk calculation methodology but also did not incorporate ISC's *Physical Security Criteria for Federal Facilities* or allow comprehensive analysis as the reports were not entered into a database.

Source: GAO analysis of FPS data.

FPS Does Not Currently Assess Risks at Federal Facilities, but Multiple Agencies Are Conducting Their Own Assessments

FPS Is Not Completing Risk Assessments

In the absence of RAMP, FPS currently is not assessing risk at the over 9,000 federal facilities under the custody and control of GSA in a manner consistent with federal standards such as *NIPP's* risk management framework, as FPS originally planned. As a result, FPS has accumulated a backlog of federal facilities that have not been assessed for several years. According to FPS data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012. However, we were unable to determine the extent of the FSA backlog because we found FPS's FSA data to be unreliable. Specifically, our analysis of FPS's December 2011 assessment data showed that 9 percent—or nearly 800—of the approximately 9,000 facilities did not have a date for when the last FSA was completed. According to the *NIPP*, to be considered credible a risk assessment must specifically address the three components of risk: threat, vulnerability, and consequence. We have reported that timely and comprehensive risk assessments play a critical role in protecting federal facilities by helping decision makers identify and evaluate potential threats so that countermeasures can be implemented to help prevent or mitigate the facilities' vulnerabilities.[6]

Although FPS is not currently assessing risk at federal facilities, FPS officials stated that the agency is taking steps to ensure federal facilities are safe. According to FPS officials, its inspectors monitor the security posture of federal facilities by responding to incidents, testing countermeasures, and conducting guard post inspections. In addition, since September 2011, FPS's inspectors have been collecting information

[6]GAO, *Homeland Security, Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection,* GAO-10-142 (Washington D.C.: Oct. 23, 2009).

about federal facilities, such as location, purpose, agency contacts, and current countermeasures (e.g., perimeter security, access controls, and closed-circuit television systems). According to FPS officials, inspectors have collected information for more than 1,400 facilities that will be used as a starting point to complete FPS's fiscal year 2012 assessments. However, FPS officials acknowledged that this is not a credible risk assessment that addresses threat, vulnerability, and consequence consistent with *NIPP's* risk management framework. Moreover, several FPS inspectors told us that they received minimal training or guidance on how to collect this information and expressed concern that the facility information collected could become outdated by the time it is used to complete an FSA.

Multiple Federal Agencies Are Conducting Their Own Risk Assessments

We reported in February 2012 that multiple federal agencies have been expending additional resources to conduct their own risk assessments, in part because they have not been satisfied with FPS's past assessments.[7] These assessments are taking place even though according to FPS's Chief Financial Officer, FPS received $236 million in basic security fees from federal agencies to conduct FSAs and other security services in fiscal year 2011.[8] For example, an Internal Revenue Service (IRS) official said that IRS completed its own risk assessments based on concerns about risks unique to its mission for approximately 65 facilities that it also paid FPS to assess. A Federal Emergency Management Agency (FEMA) official stated that FEMA has assessed its own facilities for several years because of dissatisfaction with the facility security levels that FPS assigned to its facilities. Similarly, Environmental Protection Agency (EPA) officials said that EPA has conducted its own assessments based on concerns with the quality and thoroughness of FPS's assessments. EPA officials noted that the agency's assessments are conducted by teams of contractors and EPA employees, cost an estimated $6,000 each, and can take a few days to a week to complete. An official from the U.S. Army Corps of Engineers told us that it duplicates FPS's assessments at some of its regional facilities because the agency follows

[7]GAO, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings and Enhance Revenue*, GAO-12-342SP (Washington, D.C.: February 2012).

[8]FPS currently charges tenant agencies in properties under GSA control a basic security fee of $0.74 per square foot per year for its security services including physical security and law enforcement activities as per 41 C.F.R. § 102-85.35.

U.S. Army force protection regulations, rather than FPS's security requirements.

GSA is also expending additional resources to assess risk. We reported in October 2010 that GSA officials did not always receive timely FPS risk assessments for facilities GSA considered leasing.[9] GSA seeks to have these risk assessments completed before it takes possession of a property and leases it to tenant agencies. An inefficient risk assessment process for new lease projects can add costs for GSA and create problems for both GSA and tenant agencies. Therefore, GSA is updating a risk assessment tool that it began developing in 1998, but has not recently used, to better ensure that it has timely and comprehensive risk assessments. GSA officials told us that in the future they may use this tool for other physical security activities, such as conducting other types of risk assessments and determining security countermeasures for new facilities. However, as of June 2012, FPS has not coordinated with GSA and other federal agencies to reduce or prevent duplication of its assessments.

FPS Lacks Reliable FSA Data

In addition to not having a tool that allows it to conduct risk assessments, FPS does not have reliable FSA data, which has hampered the agency's ability to manage its FSA program. For example, as mentioned previously, we found that 9 percent—or nearly 800—of the approximately 9,000 facilities in FPS's dataset were missing a date for the completion of their last FSA, thus raising questions about whether facilities have been assessed as required.[10] Additionally, we found that FPS does not have reliable and timely information regarding when inspectors provided FSA reports to tenant agencies. This information is important because federal tenant agencies rely on these reports to allocate funding for new countermeasures.

We also found that FPS's reliance on its 11 regional offices to maintain FSA data has contributed to inconsistency among the regions. For example, each of the three regions we visited maintains FSA data in a different format. More specifically, each of the three regions collected

[9]GAO-10-142.

[10]The ISC recommends that level I and II facilities be assessed every 5 years and level III and IV facilities be assessed every 3 years.

similar information such as a facility's identifier and address, but they differed in how they tracked FSAs. For example, one region tracked the dates an FSA was submitted, reviewed, and completed. Another region tracked only the date the FSA was completed. Separately, another region used multiple spreadsheets to track FSAs. These inconsistencies among the regions make it difficult to understand whether FPS can manage its FSA program nationwide.

In March 2012, DHS's Inspector General (IG) also reported similar issues with FPS's data.[11] The IG found that FPS had not determined if any of the FSA data in RAMP were valid and thus needed to be preserved for future use. As a result, the IG stated that FPS risked incurring additional expenditures, including paying for the transfer of useless data or losing critical data, if it did not make a decision before June 2012, when its data maintenance contract expired. The IG recommended that FPS (1) identify the costs and benefits of two potential courses of action: maintaining the data in RAMP or transferring the data out of RAMP, and (2) review RAMP's data to determine what was critical and what should be saved. FPS concurred with this recommendation and plans to take action.

FPS Efforts to Develop a Risk Assessment Tool Are Evolving, but Challenges Remain

FPS Has Developed an Interim Vulnerability Assessment Tool

In September 2011, FPS signed an inter-agency agreement with Argonne National Laboratory for about $875,000 to develop MIST by June 30, 2012.[12] According to FPS's MIST documentation, MIST is an interim vulnerability assessment tool that FPS plans to use until it can develop a permanent solution to replace RAMP. According to FPS officials, among

[11]Department of Homeland Security, Office of the Inspector General, *FPS' Exercise of a Contract Option for the Risk Assessment and Management Program*, OIG-12-67 (Washington, D.C.: March 2012).

[12]As of March 2012, FPS's total life cycle cost for MIST was estimated at $5 million.

other things, MIST will enable the agency to begin aligning its FSA process with *NIPP's* risk management framework and ISC standards. In addition, according to FPS's MIST documentation, MIST will address key shortcomings identified with the RAMP development effort, including lack of inspector involvement, limited testing, and an inadequate training program.[13]

According to MIST project documents and FPS officials, among other things, MIST will also:

- allow FPS's inspectors to review and document a facility's security posture, current level of protection, and recommend countermeasures;
- provide FPS's inspectors with a standardized way for gathering and recording facility data; and
- allow FPS to compare a facility's existing countermeasures against the ISC countermeasure standards based on ISC's predefined threats to federal facilities (e.g., blast-resistant windows for a level IV facility) to create the facility's vulnerability report).[14]

In addition, according to FPS officials, after completing the MIST vulnerability assessment, inspectors will use additional threat information gathered outside of MIST by FPS's Threat Management Division and any local crime statistics to justify any deviation from the ISC-defined threat levels in generating a threat assessment report. FPS plans to issue the facility's threat and vulnerability reports along with any countermeasure recommendations to the federal tenant agencies.

FPS officials stated that MIST provides several potential improvements over its prior assessment tools: FSRM, RAMP, and the FSA calculator and template. For example, in contrast to FSRM, MIST will provide a more standardized and less subjective way of both collecting facility information and recommending countermeasures. Since MIST uses the ISC recommended countermeasures for defined threat scenarios for each facility security level, FPS officials believe that MIST will increase the

[13]Federal Protective Service, *MIST Integrated Systems Logistics Plan* (Washington D.C., Mar. 27, 2012).

[14]The ISC has defined 31 different threats to federal facilities including vehicle-borne improvised explosive devices, workplace violence, and theft.

likelihood that inspectors will produce credible FSAs. In contrast, the risk scores generated by RAMP and the FSA calculator and template were not linked to ISC standards. Unlike RAMP, MIST will use a limited amount of GSA facility data that can be edited by FPS inspectors where a correction is needed, according to FPS officials. The inability to edit data in RAMP was a contributing factor to its failure to produce credible FSAs.

According to FPS officials, on March 30, 2012, Argonne National Laboratory delivered MIST to FPS on time and within budget. FPS began training inspectors on MIST and about how to use the threat information obtained outside MIST in May 2012 and expects to complete the training by the end of September 2012. According to FPS officials, inspectors will be able to use MIST once they have completed training and a supervisor has determined, based on professional judgment, that the inspector is capable of using MIST. At that time, an inspector will be able to use MIST to assess level I or II facilities. According to FPS officials, once these assessments are approved, FPS will subsequently determine which level III and IV facilities the inspector may assess with MIST.

FPS Increased Its Use of Project Management Best Practices in Developing MIST

Considered Alternatives

FPS officials said the agency completed an alternatives analysis prior to selecting MIST. We were not able to confirm this because FPS did not document its analysis. According to industry standards, documenting an alternatives analysis is important because it allows agency officials to: revisit decision rationale when changes occur, reduce the subjectivity of the decision making process, and, provide a higher probability of selecting a solution that meets multiple stakeholders' demands.[15]

FPS officials mentioned two existing tools that were considered for an interim assessment tool: NPPD's Office of Infrastructure Protection's (IP) Infrastructure Survey Tool (IST) and DHS Science and Technology Directorate's (S&T) Integrated Rapid Visual Screening of Buildings (IRVS)

[15]Carnegie Mellon University Software Engineering Institute, *Capability Maturity Model Integration for Acquisition, Version 1.2* (November 2007).

tool. FPS officials said they became aware of a security survey conducted by IP for the February 2011 Super Bowl at Cowboys Stadium in Arlington, Texas. Based on that survey, FPS reviewed the IST, which is used by IP to examine existing security countermeasures (which include physical and other protective measures) at critical infrastructure facilities, such as hydro-electric plants and commercial facilities, by comparing their existing countermeasures to those at similar facilities. According to IP officials, the IST does not calculate risk, estimate consequences, or recommend countermeasures. The IRVS is a risk assessment tool that assesses risk using threat, vulnerability, and consequence; that can be adapted to individual agency's needs; and that, according to an S&T official, was available to FPS at no cost. However, the Director of FPS decided that because of timeliness concerns and the opportunity to better share information within NPPD, FPS would develop a modified version of the IST to assess federal facilities until FPS could develop an FSA tool to replace RAMP.

Better Managed MIST's Requirements

In contrast to RAMP, FPS better managed MIST's requirements as we recommended in 2011.[16] Specifically, FPS's Director required that MIST be an FSA-exclusive tool and thus avoided changes in requirements that could have resulted in cost or schedule increases during development. Requirements serve as the basis for establishing agreement among users, developers, and customers and a shared understanding of the system being developed. Managing requirements entails managing the capabilities or conditions that a product is required to meet to satisfy an agreement or standard.

However, FPS did not obtain GSA or federal tenant agencies' input in developing MIST's requirements. We have reported that leading organizations generally include customer needs when developing programs.[17] Without this input, FPS's customers may not receive the information they need to make well-informed countermeasure decisions. FPS officials stated that they were considering getting feedback from GSA and federal tenant agencies.

[16]GAO-11-705R.

[17]GAO, *Geostationary Operational Environmental Satellites: Improvements Needed in Continuity Planning and Involvement of Key Users,* GAO-10-799 (Washington, D.C.: Sept.1, 2010).

Completed User Acceptance Testing

In March 2012, FPS completed user acceptance testing of MIST with some of its inspectors and supervisors, as we recommended in 2011.[18] User acceptance testing is conducted to ensure that a system meets contract requirements and performs satisfactorily for the user of the program—in this case, FPS's inspector workforce and their supervisors. The results of each test event need to be captured and used to ensure that any problems discovered are disclosed and corrected. We reported in 2009 that comprehensive testing that is effectively planned and scheduled can provide the basis for identifying key tasks and requirements. Testing can also better ensure that a system meets those specified requirements and functions as intended in an operational environment.[19]

According to FPS officials, user feedback on MIST was positive from the user acceptance test, and MIST produced the necessary output for FPS's FSA process. For example, the inspectors who were involved in the testing found the methodology understandable and credible and had no significant problems logging in and using MIST. FPS's testing identified the following problems: wireless connectivity issues at the testing location resulting in dropped connections and some users with older software encountering problems loading MIST onto their computers. FPS officials stated that they are taking steps to address these issues, such as updating older software.

MIST Has Limitations as an Assessment Tool

FPS has yet to decide what tool, if any, will replace MIST, which is an interim vulnerability assessment tool. According to FPS officials, the agency plans to use MIST for at least the next 18 months. Consequently, until FPS decides what tool, if any, will replace MIST or RAMP, it will continue to lack the ability to assess risk at federal facilities in a manner consistent with *NIPP*, as we previously mentioned. We also found the following limitations with MIST:

Assessing Consequence

FPS did not design MIST to estimate consequence, a critical component of a risk assessment. Assessing consequence is important because it combines vulnerability and threat information to evaluate the potential

[18]GAO-11-705R.

[19]GAO, *Information Technology: Census Bureau Testing of 2010 Decennial Systems Can Be Strengthened*, GAO-09-414T (Washington, D.C.: Mar. 5, 2009).

effects of an adverse event on a federal facility. For example, consequence information is used to determine whether a terrorist attack on a federal facility may result in the loss of human lives, incur economic costs beyond rebuilding the facility, or have an adverse impact on national security. Three of the four risk assessment experts we spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess the risks to a federal facility. As a result, while FPS may be able to identify a facility's vulnerabilities to different threats using MIST, without consequence information, federal tenant agencies may not be able to make fully informed decisions on how to best allocate resources to protect facilities.

Both FPS and ISC officials stated that incorporating consequence information into an assessment tool is a complex task. FPS officials stated that they did not include consequence information in MIST's design as it would have introduced a new component that was not part of the IST and would have taken more time to develop, validate and test, and that any changes in threats would necessitate corresponding changes to the estimated consequences. For example, if new threats to federal facilities were identified, FPS would have to modify MIST's methodology to estimate the consequences and determine how those consequences could affect other previously identified threats. FPS officials do not know if this capability can be developed in the future, but they said that they are working with the ISC and S&T to explore the possibility. However, according to an S&T official, incorporating consequence is possible and S&T's current IRVS tool does estimate consequences.

Comparing Risk across Federal Facilities

FPS did not design MIST to compare risk or assessment results across federal facilities. Consequently, FPS does not have the ability to take a comprehensive approach to risk management across its portfolio of 9,000 facilities and recommending countermeasures to federal tenant agencies. Instead, FPS takes a facility-by-facility approach to risk management. Under this approach, FPS assumes that all facilities with the same security level have the same security risk, regardless of their location.[20] However, level I facilities typically face less risk because they are generally small store-front operations with a low volume of public contact, such as a small post office or Social Security Administration Office. In comparison, a level IV facility has a high volume of public contact and

[20]GAO-10-142.

may contain high-risk law enforcement and intelligence agencies. We reported in 2010 that FPS's facility-by-facility approach to risk management provides limited assurance that the most critical risks at federal facilities across the country are being prioritized and mitigated.[21] FPS recognized the importance of having such a comprehensive approach to its FSA program when it developed RAMP and FPS officials stated that they may develop this capability for the next version of MIST.

Measuring Performance

FPS has not developed metrics to measure MIST's performance, such as feedback surveys from tenant agencies. Measuring performance allows organizations to track progress toward their goals and gives managers critical information on which to base decisions for improving their programs. We and other federal agencies have maintained that adequate and reliable performance measures are a necessary component of effective management.[22] We have also found that performance measures should provide agency managers with timely, action-oriented information in a format conducive to helping them make decisions that improve program performance, including decisions to adjust policies and priorities.[23] Without such metrics, FPS's ability to improve MIST will be hampered. FPS officials stated that they are planning to develop performance measures for MIST, but did not give a time frame for when they will do so.

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

[22]GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper its Ability to Protect Federal Facilities,* GAO-08-683 (Washington, D.C.: June 11, 2008).

[23]GAO-08-683.

FPS Faces Challenges in Overseeing Its Contract Guards

No Comprehensive System to Oversee Contract Guard Workforce

FPS does not have a comprehensive and reliable system to oversee its approximately 12,500 contract guards. In addition to conducting FSAs, FPS developed RAMP as a comprehensive system to help oversee two aspects of its contract guard program: (1) verifying that guards are trained and certified to be on post in federal facilities and (2) conducting guard post inspections.[24] However, FPS experienced difficulty with RAMP because the contract guard training and certification information in RAMP was not reliable.[25] Additionally, FPS faced challenges using RAMP to conduct post inspections. For example, FPS inspectors we interviewed stated they could not use RAMP to conduct post inspections because of difficulty connecting to RAMP's servers in remote areas and recorded post inspections disappearing from RAMP's record without explanation. Although we reported some of these challenges in 2011, FPS did not stop using RAMP for guard oversight until June 2012. Consequently, it is now more difficult for FPS to verify that guards on post are trained and certified and that inspectors are conducting guard post inspections as required.

According to FPS officials, the agency decided to no longer use RAMP for these and other reasons, including the expiration of the RAMP operations and maintenance contract in June 2012 and FPS's decision to migrate data from RAMP. In the absence of RAMP, in June 2012, FPS decided to deploy an interim method to enable inspectors to record post inspections. FPS officials said this capability is separate from MIST, does not include guard training and certification data, and will not have the ability to generate post inspection reports. In addition, FPS officials acknowledged that this method is not a comprehensive system for guard oversight.

[24]FPS's inspection requirement for FSL I and II facilities is two annual inspections of all posts, all shifts. The inspection requirement for FSL III facilities is biweekly inspections of two posts, any shift, and for FSL IV, weekly inspections of two posts, any shift.

[25]A post is a guard's area of responsibility in a federal facility.

No Independent Verification of Contract Guard Information

FPS does not independently verify the guard training and certification information provided by guard contractors. FPS currently requires its 33 guard contractors to maintain their own files containing guard training and certification information and began requiring them to submit a monthly report with this information to FPS's regions in July 2011.[26] To verify the guard companies' reports, FPS conducts monthly audits. As part of its monthly audit process, FPS regional staff visits the contractor's office to select 10 percent of the contractor's guard files and check them against the reports guard companies send FPS each month.[27]

In addition, in October 2011, FPS undertook a month-long audit of every guard file for its contracts across its 11 regions. Similar to the monthly audits, regional officials explained that the "100 percent audit" included a review of the approximately 12,500 guard files for FPS's 110 contracts to verify that guards had up-to-date training and certification information.[28] According to an FPS official, the audit was FPS's first review of all of its contractors' guard files and provided a baseline for future nationwide audits. FPS provided preliminary October 2011 data showing that 1,152 of the 12,274 guard files FPS reviewed at that time—9 percent—were deficient, meaning that they were missing one or more of the required certification document(s). However, FPS does not have a final report on the results of the nationwide audit that includes an explanation of why the files were deficient and whether deficiencies were resolved.

FPS's monthly audits provide limited assurance that qualified guards are standing post, as FPS is verifying that the contractor-provided information matches the information in the contractor's files. We reported in 2010 that FPS's reliance on contractors to self-report guard training and certification information without a reliable tracking system of its own may have

[26]For example, guard training and certifications include firearms qualification, cardiopulmonary resuscitation, First Aid, baton certification, and x-ray and magnetometer training.

[27]FPS now relies on guard contractors to keep accurate guard certification records. Each month, regional personnel are required to review 10 percent of the contractors' guard certification files to verify that the information is current and matches the monthly guard certification spreadsheet FPS receives from the contractors. According to FPS policy, if regional personnel identify deficiencies, such as expired certification documentation, in 40 percent of the files reviewed, they are to initiate an audit of 100 percent of the company's files.

[28]A guard company may have more than one contract with FPS.

contributed to a situation in which a contractor allegedly falsified training information for its guards.[29] In addition, officials at one FPS region told us they maintain a list of the files that have been audited previously to avoid reviewing the same files, but FPS has no way of ensuring that the same guard files are not repeatedly reviewed during the monthly audits, while others are never reviewed. In the place of RAMP, FPS plans to continue using its administrative audit process and the monthly contractor-provided information to verify that qualified contract guards are standing post in federal facilities.

Conclusions

FPS has taken some steps to improve its ability to assess risk at federal facilities but additional improvements are needed. Most notably, FPS has developed an interim vulnerability assessment tool that once implemented, may allow it to resume assessing federal facilities, which it has not done consistently for several years. However, FPS's lack of progress in developing a risk assessment tool that meets federal physical security standards such as *NIPP's* risk management framework is problematic for several reasons. First, FPS spent almost 4 years and $35 million dollars on RAMP and another $875,000 on MIST but still does not have a risk assessment tool that meets *NIPP's* risk management framework that can calculate risk using threat, vulnerability, and consequence information. Second, without a risk assessment tool that can compare risks across its portfolio, FPS cannot provide assurance that the most critical risks at federal facilities are being prioritized and mitigated. Third, some federal agencies are expending additional resources to conduct their own risk assessments in addition to paying FPS to complete them. Fourth, federal tenant agencies do not have critical information needed to make risk-based decisions about how to upgrade the security of their facilities. Identifying ways to resolve these issues could greatly enhance FPS's efforts to assess risk at federal facilities and reduce duplication of effort, among other things.

We recognize that MIST is an interim tool and is not yet fully implemented; however, it has limitations that could affect FPS's ability to protect federal facilities and provide security services. FPS generally increased its use of our project management best practices, as we

[29]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).

recommended, and we encourage it to continue to do so in any future development of a risk assessment tool. However, FPS has not improved the accuracy and reliability of its FSA and contract guard data as it agreed to do in response to our previous recommendation. Given that FPS is still experiencing difficulties managing its FSA data, we reiterate the importance of this prior recommendation and encourage FPS to take action to address it.

Finally, FPS recently decided to not use RAMP to oversee its contract guards, but still does not have a comprehensive and reliable system to ensure that its approximately 12,500 contract guards have met training and certification requirements, and that FPS's guard post inspections are occurring in accordance with the agency's guidelines. That FPS cannot ensure that its 33 contractors are providing accurate information on its guards is also problematic. Without a comprehensive and reliable system for contract guard oversight, FPS is relying primarily on information provided by guard companies. These issues raise important questions regarding the overall effectiveness of FPS's oversight of its contract guard workforce.

Recommendations for Executive Action

Given the challenges that FPS faces in assessing risks to federal facilities and managing its contract guard workforce, we recommend that the Secretary of Homeland Security direct the Under Secretary of NPPD and the Director of FPS to take the following five actions:

- incorporate *NIPP's* risk management framework—specifically in calculating risk to include threat, vulnerability, and consequence information—in any permanent risk assessment tool;
- coordinate with GSA and other federal tenant agencies to reduce any unnecessary duplication in security assessments of facilities under the custody and control of GSA;
- address MIST's limitations (assessing consequence, comparing risk across federal facilities, and measuring performance) to better assess and mitigate risk at federal facilities until a permanent system is developed and implemented;
- develop and implement a new comprehensive and reliable system for contract guard oversight; and
- verify independently that FPS's contract guards are current on all training and certification requirements.

Agency Comments

We provided a draft of this report to the Secretary of Homeland Security for review. DHS concurred with our recommendations and provided written comments that are reprinted in appendix II. DHS also provided technical comments that we incorporated where appropriate.

We are sending copies of this report to the Secretary of Homeland Security and the Director of the Federal Protective Service. 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 relevant congressional committees. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov. If you or your staff members have any questions concerning this report, please contact me at (202) 512-2834 or goldsteinm@gao.gov. Contact point for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff that made key contributions to this report is listed in appendix III.

Sincerely yours,

Mark L. Goldstein
Director, Physical Infrastructure Issues

Appendix I: Scope and Methodology

To examine the extent to which FPS is completing risk assessments without RAMP, we reviewed FPS's current FSA procedures and data on completed and planned FSAs for fiscal years 2010 to 2012. Specifically, we reviewed FPS's FSA data aggregated from its 11 regions to determine the extent of FPS's FSA backlog. These data included the GSA facility identifier, address, city, state, zip code, FPS region, facility security level, date of the last FSA, and the date of the next scheduled FSA. However, we could not determine the extent of FPS's FSA backlog because FPS's data contained a number of missing and incorrect values that made it unreliable. We also visited 3 of FPS's 11 regions and interviewed regional managers, area commanders, and inspectors about how they are completing FSAs in the absence of RAMP. We selected these 3 regions based on the number of federal facilities in the region and their facility security levels, the number of contract guards in the region, and geographic dispersion. Our work is not generalizable to all FPS regions. We also interviewed FPS headquarters officials to understand how the agency is currently conducting FSAs. During our visits to the selected 3 FPS regions, we spoke with officials from the General Services Administration, Department of Veterans Affairs, the Federal Highway Administration, Immigration and Customs Enforcement, and United States Citizenship and Immigration Services to obtain their perspectives on FPS's assessment efforts. These agencies were selected because they are members of their facility security committees, which have responsibility for addressing security issues at their respective facilities and approving countermeasures recommended by FPS.

To determine the status of FPS's efforts to develop an FSA tool, we reviewed FPS's documents including: the interagency agreement, requirements plan, project plan, system test plan, and training plan for MIST. As applicable, we compared FPS's efforts to develop an FSA tool to DHS's *National Infrastructure Protection Plan's* (*NIPP*) risk management framework and the Interagency Security Committee's (ISC) standards, including the *Physical Security Criteria for Federal Facilities* and the *Facility Security Level Determination for Federal Facilities*.[1] We

[1]The ISC is comprised of representatives from more than 50 federal agencies and departments, establishes standards and best practices for federal security professionals responsible for protecting non-military federal facilities in the U.S. FPS is a member agency of the Interagency Security Committee in the Department of Homeland Security, along with other federal agencies such as the General Services Administration, the Federal Aviation Administration, the Environmental Protection Agency, and other departments within the Department of Homeland Security.

examined FPS's requirement and project documents to determine whether in developing MIST, FPS complied with selected GAO and industry project-management best practices, such as: conducting alternative analysis, managing requirements, and conducting user acceptance testing. These practices were selected because they are critical in developing information technology systems and we recommended in 2011 that FPS better manage its requirements and conduct user acceptance testing in developing future tools. We interviewed FPS headquarters and regional officials as well as inspectors, representatives from Argonne National Laboratory who are responsible for developing MIST, officials from NPPD's Office of Infrastructure Protection, and four risk management experts. We selected our four risk assessment experts from a list of individuals who participated in the Comptroller General's 2008 risk management forum.[2] We interviewed these experts to discuss FPS's efforts to assess risks to federal facilities and the benefits and challenges of a risk assessment.

To assess FPS's effort to manage its contract guard workforce, we reviewed FPS's guard oversight policies and procedures and RAMP's September 30, 2011, post inspection data. During our visits to the selected three FPS regions, we interviewed FPS regional managers, area commanders, inspectors, three guard contractors, GSA, and other federal agencies about guard oversight. We also interviewed officials at FPS's headquarters.

We conducted this performance audit from July 2011 through August 2012 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.

[2]GAO, *Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-627SP (Washington, D.C.: April 2008).

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

July 19, 2012

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

Re: Draft Report GAO 12-739, "FEDERAL PROTECTIVE SERVICE: Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities"

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 was pleased to note GAO's positive recognition of the National Protection and Programs Directorate (NPPD)/Federal Protective Service's (FPS's) Modified Infrastructure Survey Tool (MIST) and better use of project management best practices in its development. During the development, FPS continuously monitored the security posture of federal facilities by responding to incidents, testing countermeasures, and conducting guard-post inspections. FPS inspectors captured critical information relative to their assigned facilities on Pre-MIST Worksheets. This information will be used to assess vulnerabilities and complete Facility Security Assessment (FSA) reports once the MIST tool is fully deployed. To date, more than 1,400 Pre-MIST worksheets have been completed. However, through the Risk Assessment and Management Program experience, FPS has learned that having just a single tool or application to manage its varied operational functions is not currently the most appropriate solution. Specifically, it is important to note that more than one tool may be necessary to comprehensively conduct FSAs and oversee the Protective Security Officer (PSO) program.

According to GAO, MIST is not fully compliant with DHS's National Infrastructure Protection Plan's (NIPP) risk management framework, specifically with regard to comparing risk across facilities. While FPS performs its operations as part of the NIPP Sector Partnership Framework, it has additional requirements to meet Interagency Security Committee (ISC) standards for federal facility security, which are facility specific. MIST does not compare assessment results across federal facilities in an individual FSA report. It considers each facility's unique security concerns and compares the security posture against a baseline protective measure index for the specific Facility Security Level as defined within the ISC standard, "Physical Security Criteria for Federal Facilities." Over time, the data gathered in MIST will permit aggregation and

analysis to enable identification of security and protection gaps for mitigation across categories such as Facility Security Levels and tenant agencies, where appropriate to do so.

Notably, NPPD/FPS incorporated better use of GAO project management best practices in its development of MIST, as recommended by GAO in 2011[1]. Specifically, NPPD/FPS completed an alternatives analysis prior to selecting MIST; required that MIST be an FSA-exclusive tool, thus avoiding potential requirement changes that could have resulted in cost or schedule increases; and successfully completed user acceptance testing of MIST with FPS's inspector workforce and their supervisors. Feedback from the user acceptance test was positive, and MIST produced the necessary output for FPS's FSA process. FPS continues to deploy MIST and is in the process of training its Inspector cadre on the tool.

The draft report contained five recommendations, with which DHS concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the Under Secretary of NPPD and the Director of FPS to:

Recommendation 1: Incorporate the NIPP risk management framework—specifically in calculating risk to include threat, vulnerability, and consequence information—in any permanent risk assessment tool.

Response: Concur. NPPD/FPS designed MIST as a vulnerability assessment tool and therefore did not include threat or consequence calculations within the requirements. Using modular development, future efforts will incorporate these aspects of risk, as defined by the NIPP, within this interim tool. NPPD/FPS plans to coordinate with the ISC to clarify certification requirements for risk management tools, and the implications of a return on investment for developing a tool that incorporates all necessary components for risk-based decisions.

In the meantime, the threat assessment component of the FSA is currently being completed by field Regional Intelligence Agents (RIAs) and reported as part of the final FSA. RIAs have received training on their role in the threat assessment process, which covers not only the intelligence-based threat picture, but also local criminal activity and threats that should be considered when countermeasures are assessed. In addition, some consequence assessment is included in the ISC's Facility Security Levels that FPS currently applies. For example, they consider the number of employees, whether the facility is near a popular tourist destination, and the scope of services that the facility provides.

FPS will also seek to further align future operational activities to incorporate the tenets of the NIPP's risk management framework, which are: Set Security Goals, Identify Assets and Functions, Assess Risks, Prioritize, Implement Protective Programs, and Measure Effectiveness.

Recommendation 2: Coordinate with GSA and other Federal tenant agencies to reduce any unnecessary duplication in security assessments of facilities under the custody and control of GSA.

---

[1] GAO, *Federal Protective Service: Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS's Risk Assessment and Management Program,* GAO-11-705R (Washington, D.C.: July 15, 2011).

Response: Concur. Working closely with the General Services Administration, FPS will continue to coordinate with other federal agencies to reduce any potential duplication of efforts in producing independent security assessments. In the fall of 2011, FPS requested and GSA agreed to assign a full-time GSA senior liaison to FPS headquarters. Together, FPS and GSA have been interacting and addressing this issue and plan to engage the ISC and the Federal Facilities Sector, which they co-lead, to discuss the issue. While FPS has no authority to preclude any agency from producing a work product of their choosing, we will continue to provide agencies with ongoing and cyclical security assessments as required.

Recommendation 3: Address MIST's limitations (assessing consequence, comparing risk across Federal facilities, and measuring performance) to better assess and mitigate risk at Federal facilities until a permanent system is developed and implemented.

Response: Concur. As discussed in the response to Recommendation 1, FPS will employ modular development to incorporate the threat and consequence aspects of risk analysis with a facility security assessment tool. Performance metrics for the MIST have been identified, and plans have been made to engage with Facility Security Committees to gather feedback on the implementation of the FSA process and reporting requirements. Feedback that can be appropriately addressed by MIST will be considered as part of future enhancements.

Recommendation 4: Develop and implement a new comprehensive and reliable system for contract guard oversight.

Response: Concur. As noted by GAO, FPS is not currently resourced to begin the development of a system or other technological applications to enable more efficient and comprehensive oversight of a program as large in scope as the PSO program. Therefore, NPPD/FPS is also working with DHS's Science and Technology Directorate to address GAO's recommendations concerning a system for contract guard oversight and explore means of leveraging technology to ensure effective oversight of PSOs, such as automated tracking of the manning of guard posts and PSO possession of the necessary credentials to stand post.

Recommendation 5: Independently verify that FPS's contract guards are current on all training and certification requirements.

Response: Concur. FPS currently provides contract oversight to include independent verification of contract guard information using a variety of methods. While FPS does not employ a 100-percent verification rate, the policy and procedures currently in place are sufficient to gain reasonable assurance of contract compliance and to identify significant performance problems or negative trends for resolution.

FPS requires its PSO vendors to train and certify PSOs as specifically set forth in the contract. Initially, and monthly thereafter, vendors self-certify/validate each contract guard's training and certification, ensuring they meet all FPS requirements prior to standing post. In accordance with the Statement of Work, vendors are required to (1) maintain copies of all certification and training certificates and licenses in a personnel folder for each guard, and (2) execute and provide Training and Quality Control Plans and a monthly training/certification spreadsheet to

3

FPS, demonstrating compliance with the contract and providing FPS information to aid in contract oversight.

FPS conducts monthly Administrative Audits, auditing 10 percent of total guard force (personnel files), per contract. If a deficiency rate of 40 percent or more occurs during any audit period, a 100 percent audit is conducted as soon as possible. Those PSOs identified as not properly trained/certified are not authorized to stand post until contractual requirements are met. FPS also has authority to direct vendors to produce PSO personnel files at any time for review. Additionally, FPS Directive 15.9.1.3, Contract Protective Security Force Performance Monitoring, Section 6.2, Post Inspections, allows FPS representatives conducting post inspections to verify guard training/qualifications during personal interaction between FPS representative and PSOs. Finally, Section 6.5, Monitoring of Contractor Provided Training and Weapons Qualifications, requires FPS personnel to monitor all weapons qualifications, a minimum of 16 hours of each initial basic training program, and a minimum of 8 hours of each recurring refresher course.

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
Director
Departmental GAO-OIG Liaison Office

4

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Tammy Conquest, Assistant Director; Geoffrey Hamilton; Greg Hanna; Grant Mallie; Justin Reed; Amy Rosewarne; and Frank Taliaferro made key contributions to this report.