United States Government Accountability Office

GAO

Report to Congressional Requesters

August 2012

CRITICAL INFRASTRUCTURE

DHS Needs to Refocus Its Efforts to Lead the Government Facilities Sector

GAO-12-852

August 2012

CRITICAL INFRASTRUCTURE

DHS Needs to Refocus Its Efforts to Lead the Government Facilities Sector

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-852, a report to congressional requesters

Why GAO Did This Study

U.S. government facilities have been the target of foreign and domestic terrorists. Government facilities are one of 18 critical infrastructure sectors designated under Homeland Security Presidential Directive 7 (HSPD-7). The Department of Homeland Security (DHS) is responsible for identifying, prioritizing, and coordinating the protection of critical infrastructure that, if destroyed, could have a debilitating impact on governance, the economy, national morale, or public health and safety. DHS defines critical infrastructure sector responsibilities in the National Infrastructure Protection Plan (NIPP) and the Federal Protective Service (FPS) is the lead agency for the government facilities sector. As such, FPS is to develop and implement a government facilities sector-specific plan, which was first issued in 2007 and updated in 2010, in coordination with governmental partners. In this report, GAO assesses FPS's efforts as the lead agency for the government facilities sector. To do this, GAO reviewed HSPD-7, the NIPP, the 2010 plan and other related documents to compare FPS's actions and the goals for the sector. GAO also interviewed DHS agency officials and 16 selected sector partners about activities for, and coordination with, the sector.

What GAO Recommends

GAO recommends that the Secretary of DHS direct FPS, in partnership with others, to develop and publish an action plan that identifies sector priorities and resource requirements, and addresses steps needed to implement a risk management approach and develop effective partnerships. DHS concurred with the recommendation.

View GAO-12-852. For more information, contact Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

The Federal Protective Service (FPS) has not been effective as the lead agency for the government facilities sector, which includes facilities at the federal, state, local, tribal and territorial level. Under the National Infrastructure Protection Plan (NIPP) and the 2010 sector-specific plan, FPS is responsible for establishing a risk management approach and developing effective partnerships for the sector. However, FPS has not implemented a risk management approach. According to FPS, it has not identified or obtained data on facilities at the federal, state, local, tribal and territorial level, which are fundamental for employing a risk management approach. In addition, despite providing information on the principles of threat, vulnerability, and consequence, FPS has not coordinated or assessed risk across government facilities, another key element of risk management. FPS also lacks effective metrics and performance data to track progress toward implementing a risk management approach and for the overall resilience or protection of government facilities. Consequently, FPS does not have a risk management approach for prioritizing and safeguarding critical government facilities. Furthermore, FPS has not built effective partnerships across different levels of government. While FPS chairs the Government Coordinating Council (the Council)—a mechanism intended to help share activities and policy across different levels of government—the Council's membership lacks a full spectrum of sector partners, particularly non-federal. All five state and local government and non-governmental members of the Council that GAO contacted were unaware of, or did not consider themselves to be part of, the Council. FPS also has not leveraged the State, Local, Tribal and Territorial Government Coordinating Council, an existing mechanism to coordinate with non-federal government organizations, although FPS officials reported recent efforts aimed at enhancing this partnership.

As the lead agency for the sector, FPS faces challenges associated with funding and its lack of an action plan. According to FPS officials, FPS has no dedicated line of funding for its activities as the lead agency and resource constraints hinder FPS's capacity to lead this large and diverse sector, which is comprised of more than 900,000 federal assets, as well as assets from 56 states and territories; over 3,000 counties; 17,000 local governments; and 564 federally recognized tribal nations. FPS's use of fee-based revenue to perform homeland security activities not directly related to federal facility protection is inconsistent with the Homeland Security Act of 2002. FPS does not have a full understanding of the resource requirements for serving as the lead agency, because it has not completed a cost estimate or an action plan to guide implementation of the 2010 plan. According to DHS officials, HSPD-7 will be updated, which may result in structural changes to the sector that could affect the lead agency's responsibilities and available resources. An action plan could serve as a valuable tool for FPS and DHS to identify priorities that can be feasibly achieved and the resources required, in tandem with any potential structural changes.

Contents

Abbreviations

DHS	Department of Homeland Security
FPS	Federal Protective Service
GSA	General Services Administration
HSPD-7	Homeland Security Presidential Directive 7
IP	Office of Infrastructure Protection
ISC	Interagency Security Committee
NIPP	National Infrastructure Protection Plan
RAMP	Risk Assessment and Management Program
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 13, 2012

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

The Honorable Sheila Jackson Lee
Ranking Member
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

Foreign and domestic terrorists have targeted U.S. government facilities, including the 1995 Oklahoma City bombing, 1998 embassy bombings in East Africa, and 2001 attack on the Pentagon. More recent incidents at government facilities include shootings at a federal courthouse in Las Vegas and the state capitol of Texas. Government facilities are 1 of 18 critical infrastructure sectors designated under Homeland Security Presidential Directive 7 (HSPD-7), which is designed to identify, prioritize, and coordinate protection of critical infrastructure.[1] Critical infrastructure is defined as systems and assets, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on governance, the economy, national morale, or public health and safety. HSPD-7 defines critical infrastructure sector responsibilities for the Department of Homeland Security (DHS) and other federal agencies that lead coordination within and across the 18 sectors. As the lead agency for the government facilities sector, DHS is responsible for working with various partners—including other federal agencies; state, local, tribal, and territorial governments as well as other sectors—to develop and implement the government facilities sector-specific plan, which was last updated in 2010 (the 2010 plan), and issue annual reports on the status of DHS's efforts.

[1]The 18 sectors are Food and Agriculture; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Transportation Systems; and Water.

DHS has designated the Federal Protective Service (FPS) as the lead agency for the government facilities sector—a collateral duty to FPS's traditional role protecting over 9,000 owned or leased federal facilities under the custody and control of the General Services Administration (GSA). FPS employs about 1,225 federal staff and oversees about 14,000 contract security guards. Over the last decade, FPS has experienced well-documented management and funding challenges that have hampered its ability to protect federal facilities. Furthermore, we have reported on gaps and overlap with respect to DHS's efforts to protect critical infrastructure.[2]

You asked us to assess DHS's activities related to the government facilities sector; particularly FPS's leadership of the sector. To meet this objective, we reviewed HSPD-7, DHS's National Infrastructure Protection Plan (NIPP), and the 2010 plan. Based on these documents, we identified the implementation of a risk management approach and development of effective partnerships as two key activities that lead agencies are responsible for. We also reviewed the 2010 and 2011 sector annual reports to identify what actions FPS had taken, and any gaps between these actions and the stated goals and activities in the 2010 plan. We interviewed DHS and FPS officials, and selected 16 of the 26 members of the Government Facilities Sector Government Coordinating Council (the Council) —a collaborative body, which shares approaches to infrastructure protection. We chose Council members based on their significant involvement within the sector, among other criteria, as well as all 5 state, local, and non-governmental members. Lastly, we reviewed our prior reports and DHS Office of Inspector General reports on critical infrastructure to identify any challenges FPS faces in leading the implementation the 2010 plan. See appendix I for a detailed description of our scope and methodology.

We conducted this performance audit from December 2011 to 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

[2]Recent GAO products on FPS and critical infrastructure protection are listed at the end of this report.

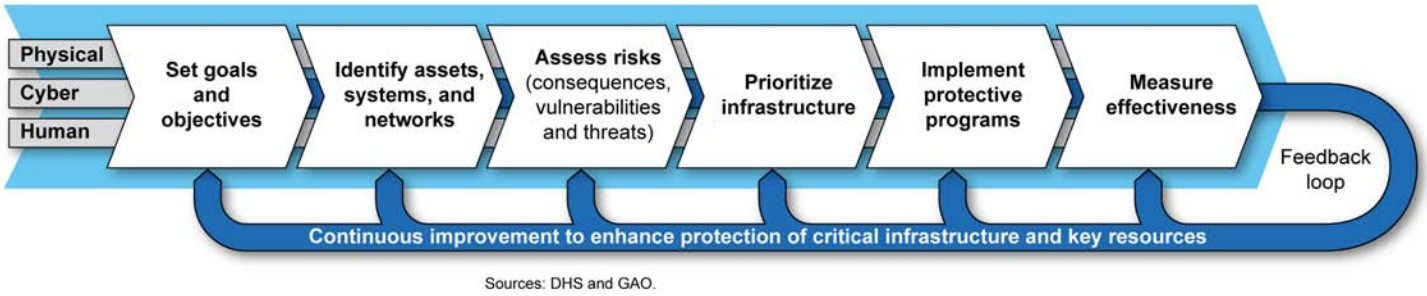
that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In 2003, HSPD-7 established a national policy for critical infrastructure and key resources. HSPD-7 designated DHS as the agency responsible for coordinating the nation's efforts to protect critical infrastructure. The Office of Infrastructure Protection (IP) within DHS fulfills the functions associated with managing and coordinating the national protection efforts. In June 2006, DHS issued the first NIPP as required by HSPD-7. The NIPP provides a risk management framework and sector partnership model for developing, implementing, and maintaining a coordinated national effort to manage the risks to critical infrastructure.

FPS is the lead agency for the government facilities sector (the sector), and assumes multiple roles and responsibilities for the sector, which is comprised of a wide variety of facilities and assets owned or leased by federal, state, local, tribal, or territorial governments, located both domestically and overseas.[3] Under the NIPP risk management framework, FPS is responsible for leading and coordinating six major elements sector-wide to identify, prioritize, and measure progress towards protecting critical infrastructure. See figure 1.

Figure 1: Six Major Elements of Identifying, Prioritizing, and Measuring Critical Infrastructure Protection



Sources: DHS and GAO.

[3]Some types of government facilities are exclusive to the sector, while other facilities exist in other sectors. Unlike other sectors, the government facilities sector does not include private sector participation. The government facilities sector also includes one subsector, the education facilities subsector, which represents both public and private educational institutions from pre-kindergarten through higher education. The Department of Education serves as the lead agency for the education facilities subsector and is responsible for developing and implementing a sector-specific plan in coordination with FPS. However, our work did not focus on the activities associated with this subsector.

Additionally, the NIPP sector partnership model calls on FPS to form and chair a government coordinating council comprised of representatives from different levels of government to share activities, policy, and communications.[4] FPS also participates in or interacts with the following cross-sector councils, which facilitate relationships within and among the 18 sectors:

- The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), which coordinates with non-federal government organizations across all 18 sectors;
- the Regional Consortium Coordinating Council, which represents a variety of distinct collaborative efforts between state, local, and private sector partners focused on critical infrastructure found in multistate regions or within a given city;
- the NIPP Federal Senior Leadership Council, which is a DHS-chaired council that consists of federal department and agency representatives from lead agencies named in HSPD-7; and
- the Critical Infrastructure Partnership Advisory Council, which is a partnership between government and private sector owners and operators of critical infrastructure to effectively coordinate federal protective programs.

The NIPP requires each lead agency to develop and revise a sector-specific plan that addresses critical infrastructure protection. FPS has responsibility for updating the plan to adequately represent the sector and involve Council members. Every 4 years,[5] FPS must:

- identify gaps between the plan and guidance from IP, policy changes, and best practices;

[4]The NIPP sector partnership model also encourages the formation of a sector coordinating council comprised of owners and operators, generally from the private sector. The sector coordinating council and the government coordinating council are intended to work in tandem to create a coordinated national framework for protection of critical infrastructure and resiliency across sectors. However, due to the governmental nature of the sector, the sector does not have a corresponding sector coordinating council.

[5]In 2012, IP changed the requirement for updating sector-specific plans from 3 years to 4 years.

- identify and develop a consolidated list of actions required to close gaps;
- obtain, and incorporate input from sector partners and the Council in multiple rounds; and
- obtain final approval from IP and release the plan to sector partners and the Council.

FPS and DHS issued the first sector-specific plan in 2007 and an update to the plan in 2010, in which they identified goals and objectives for the sector, shown in table 1.

Table 1: Sector's Stated Goals and Objectives

Goal	Objectives
1. Implement a long-term government facility risk management program	• Identify and obtain appropriate data for facilities located domestically and overseas • Coordinate a comprehensive risk assessment program for these facilities • Build effective protective measures, programs, strategies, and related guidance • Monitor performance • Develop best practices and guidance for countermeasures
2. Organize and partner for government facility protection and resilience	• Understand and share information about threats and hazards • Build effective sector partnerships for information-sharing and to help implement protection and resilience programs • Coordinate the development of continuity programs
3. Integrate government facility protection as part of the homeland security mission	• Integrate sector efforts with other national level efforts to deal with risk
4. Manage and develop the capabilities of the sector	• Promote awareness, education, training, and exercise programs • Conduct research and development • Develop and maintain the sector-specific plan
5. Maximize efficient use of resources for government facility protection	• Determine the sector priorities, program requirements, and funding needs for government facility protection • Enable or augment protection for nationally critical government facilities and coordinate efforts of sector partners and pooling of different funding sources.

Source: FPS and DHS, 2010 Government Facilities Sector-Specific Plan.

As the lead agency, HSPD-7 also requires FPS to provide the Secretary of Homeland Security with annual reports to assess progress and effectively prioritize sector-specific activities and gaps, among other things. This process involves consulting the Council, similar to the 2010 update to the plan.

FPS's role as the lead agency for the sector is an additional duty beyond its traditional role of protecting over 9,000 owned or leased facilities under the custody and control of GSA.[6] As part of its mission, FPS conducts risk assessments, recommends countermeasures, and performs law enforcement activities, such as incident response. FPS's activities are funded by security fees collected from tenant federal agencies. As such, FPS charges each tenant agency a basic security fee per square foot of space occupied in a GSA facility, among other fees.[7]

The Interagency Security Committee (ISC), which was established in 1995, develops policies and standards and facilitates security-related information exchanges. While domestic non-military federal facilities—whether federally owned, leased, or managed—are required to adhere to the ISC standards, these standards do not apply to state, local, tribal, and territorial government facilities. ISC membership consists of over 100 senior executives from 51 federal agencies and departments, including FPS. DHS is responsible for chairing the ISC and is authorized to monitor federal agencies' adherence to ISC standards.

FPS Is Not Effectively Leading the Sector

FPS's leadership has not resulted in implementation of a risk management approach for the sector, as called for under the NIPP framework. Specifically, a lack of facilities data, risk assessments, and effective metrics and performance data undermine the implementation of a risk management approach. Under FPS's leadership, effective partnerships have also not developed. FPS faces challenges in leading the sector linked to the sector's size, diversity, and FPS's fee-based revenue structure. These challenges are compounded by the lack of an action plan.

[6]Section 1315(a) of Title 40, United States Code, provides that: "To the extent provided for by transfers made pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security…shall protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property."

[7]FPS's enacted budget authority for fiscal year 2012 was $1.285 billion.

No Overarching Risk Management Approach in Place

Lack of facilities data: Asset identification is a crucial element for risk management as outlined by both the NIPP framework and the 2010 plan. According to the 2010 plan, the sector's assets and systems must be identified to determine which of these, if damaged, would result in significant consequences for national economic security, public health or safety, morale, or governance. The 2010 plan also states that identifying and obtaining appropriate data on government facilities located domestically and overseas is a sector objective. However, FPS officials said that they have not identified or obtained data on federal, state, local, tribal and territorial government facilities for the sector. According to FPS officials, developing sector-wide data may be untenable and unwarranted, because most federal, state, local, tribal, and territorial government facilities do not meet the threshold established by IP for the most critical infrastructure and government facilities generally remain the same year after year.[8] Yet, the 2010 plan states that several circumstances may require frequent updates to data on government facilities, including changes in threat levels, large-scale facility renovations, or the identification of a facility as supporting a nationally critical function or critical asset. Moreover, the 2011 annual report states that functions carried out in one government facility often directly support the functions under way in many other government facilities. Thus, an incident at one facility could have cascading impact across a range of functions essential to governance. Without appropriate data on government facilities, FPS has limited awareness of the potentially evolving universe of government facilities as well as the interdependencies that may exist in the sector. As a result, FPS may be overlooking facilities whose failure or degradation could pose significant harm to the nation's security, health, economy, or morale.

While FPS officials said that they have neither identified nor obtained data on the sector, FPS has contributed to the development of a database maintained by IP, the IP Gateway / Infrastructure Information Collection

[8]DHS has established a National Critical Infrastructure Prioritization Program with a tiered approach to identify critical infrastructure that if destroyed or disrupted, could cause some combination of significant casualties, major economic loss, or widespread and long-term disruptions to national well-being and governance capacity. The categorization of level 1 and level 2 provide a basis on which DHS and its partners can implement protection programs.

System.[9] IP uses this database to identify critical infrastructure assets and systems. According to FPS officials, they periodically review and cross reference the information contained within the database against the dataset that FPS uses as part of its role of protecting federal facilities. However, FPS's data do not encompass the full spectrum of sector facilities, in particular non-federal facilities. In addition, we have previously identified problems with FPS's data, such as a lack of data on building jurisdictional authorities.[10] Consequently, FPS's efforts to corroborate the data contained within the IP Gateway / Infrastructure Information Collection System are undermined by the limited scope and quality of its data.[11] To the extent that the IP Gateway / Infrastructure Information Collection System is used to prioritize critical infrastructure, this effort may also be detrimentally affected by weaknesses in FPS's data.

No sector-wide risk assessments: FPS is not currently positioned to assess risk across the sector. Assessing risks and coordinating risk assessment programs are another key element of the NIPP framework and a sector objective. The plan and annual reports provide information about the principles of threat, vulnerability, and consequence as well as discuss different types of risks and threats faced by government facilities, but no standardized tool for performing risk assessments exists at the federal level, much less the state, local, tribal, and territorial levels.[12] FPS

[9]The IP Gateway / Infrastructure Information Collection System, formerly referred to as the Infrastructure Data Warehouse, catalogs the national inventory of assets, systems, and networks that may be critical to the Nation's well-being, economy and security and is maintained by DHS. It provides a framework to access and display descriptive data on critical infrastructure submitted by federal, state, and local agencies; the private sector; and integrated federal or commercial databases. FPS officials said that they helped develop a taxonomy to standardize the categorization of facilities and group critical infrastructure by sector in order to identify overlaps and interdependencies across sectors, which is used within the IP Gateway / Infrastructure Information Collection System.

[10]GAO, *Federal Protective Service: Better Data on Facility Jurisdictions Needed to Enhance Collaboration with State and Local Law Enforcement,* GAO-12-434 (Washington, D.C.: Mar. 27, 2012).

[11]We have ongoing work looking at the data collection and reliability across the 18 sectors.

[12]A variety of tools are used by government agencies to assess risks. For example, according to DHS officials, DHS's Science and Technology Directorate has developed a tool called the Integrated Rapid Visual Screening, which has been used by federal, state, and local government agencies to assess risks. However, according to FPS, this tool was not built to meet FPS or sector requirements. Nonetheless, FPS has not coordinated the use of any tools to assess risk across the sector.

promoted its Risk Assessment and Management Program (RAMP) as a risk assessment tool in the 2010 plan and sector annual reports, as well as in past Council meetings. However, the scope of RAMP was not originally intended to address non-federal facilities and has never become fully operational. Therefore, its usefulness as a sector-wide risk assessment tool is not clear. In fact, RAMP has been terminated according to a senior FPS official, and FPS is working on developing a replacement.[13] According to this official, a new risk assessment tool and methodology will be released for use by sector partners at a future, unspecified date. FPS officials acknowledged the absence of a sector-wide risk assessment. Without this, FPS cannot prioritize facilities or implement protective programs, both activities predicated on effective risk assessment.[14]

No effective metrics and performance data: FPS has not established effective metrics and performance data, which hampers its ability to monitor the sector's progress toward the sector goal of implementing a long-term government facility risk management program as described in the 2010 plan. An effective metric is one that can adequately indicate progress toward a goal and that is objective, measureable, and quantifiable. Data to track metrics need to be sufficiently timely, complete, accurate, and consistent.[15] Further, DHS has established guidance on metrics to assess improvements in the protection and resiliency of critical infrastructure, which lead agencies can use to guide these efforts in their respective sectors. We have reported that without effective performance data, decision makers may not have sufficient information to evaluate whether investments have improved security and reduced a facility's

[13]We have previously reported that FPS has struggled to operationalize RAMP. 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).

[14]According to IP officials, IP has produced reports summarizing the protective activities used within each sector, including the government facilities sector, to monitor and help mitigate risks. According to FPS officials, they reviewed this report for situational awareness, but not for planning purposes or to mitigate risks, because it summarized protective measures implemented at only 91 facilities in the sector, a very small fraction of the total facilities.

[15]GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act,* GAO/GGD-96-118 (Washington, D.C.: June 1, 1996); GAO, *Managing for Results: Challenges in Producing Credible Performance Information,* GAO/T-GGD/RCED-00-134 (Washington, D.C.: Mar. 22, 2000).

vulnerability, or to determine funding priorities within and across agencies.[16]

To measure overall critical infrastructure protection or resilience within the sector, FPS identified 10 key activities that seek to reduce risk and enhance the sector's overall security posture. However, all of these risk mitigation activities are focused solely on individual federal activities or facilities, which limit their usefulness for measuring progress sector-wide. For example, to measure its implementation of a long-term government facility risk management program, FPS identified 2 risk mitigation activities focused on completing timely and thorough building assessments and implementing security support services at MegaCenters,[17] services performed by FPS as part of its mission. While these ongoing efforts may contribute to the security efforts for facilities that FPS protects, they do not provide a risk management program for the sector. Moreover, although FPS has identified metrics for each risk mitigation activity, the corresponding performance data needed to track these metrics do not exist in several cases. For example, one risk mitigation activity aims to promote the development and implementation of the ISC security standards; the associated metric identified is the number of facilities that have implemented the ISC standards. According to the ISC executive director, there is currently no way to quantify how many facilities have implemented the ISC standards.

FPS officials stated that it is difficult to identify metrics or performance data that effectively indicate progress in the sector. In addition, FPS officials said that the risk mitigation activities they identified are interim measures and that they continue to refine the sector's metrics and data. In 2011, FPS used qualitative statements to describe activities and progress made in the sector. However, these statements do not have associated outcome metrics or performance data that can be validated in

[16]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).

[17]In 2000, FPS transitioned all alarm-monitoring and dispatching capabilities from several regional control centers to four MegaCenters. Currently, each MegaCenter monitors multiple types of alarm systems, closed circuit television, and wireless dispatch communications within federal facilities throughout the nation. These centers—located in Michigan, Colorado, Pennsylvania, and Maryland—are equipped with state-of-the-art communication systems and operate continuously.

terms of timeliness, completeness, accuracy, or consistency. Until it establishes quantifiable metrics and performance data, FPS will be unable to gauge progress toward implementing a risk management approach, specifically, and the protection or resiliency of critical government facilities, overall.

FPS Has Not Built Effective Partnerships across Different Levels of Government

To effectively implement the NIPP and achieve the goals of the sector, partnerships are essential. As previously discussed, the NIPP sector partnership model integrates partners into the planning and operational activities for a collaborative approach to the protection of critical infrastructure. Likewise, the 2010 plan places a significant emphasis on the role of partnerships. However, of the 16 Council members we contacted, 13 indicated that they had little or no involvement in developing the sector plan and annual reports, and for at least 8 agencies these documents were of negligible value. To offset low Council member response, FPS officials reported relying on open source information (e.g., annual federal budget) to develop the annual report. Relying primarily on open source information does not fully or effectively leverage the knowledge and experience of Council members, potentially undermining the value of the plan as a means to promote collaboration in critical infrastructure protection.[18] Consequently, this key coordination goal of the 2010 plan has not been met, and as a result, FPS is limited in its ability, as lead agency for the sector, to productively contribute to the larger DHS effort to prioritize and safeguard the nation's most critical infrastructure. FPS's role as lead agency for the government facilities sector is particularly critical because according to the 2011 annual report, government facilities have been the most frequently attacked sector since 1968 and the sector involves a very dynamic threat environment. FPS's compilation of reports that hold little value for sector partners, leaves FPS and its sector partners less able to engage in a comprehensive risk management framework that addresses this threat environment.

Furthermore, while FPS chairs the Council, the principle mechanism for engaging partners, FPS has not involved the full spectrum of sector

[18]GAO has defined key practices to enhance and sustain collaboration among governmental partners, including establishing joint strategies to help align partner agencies' activities and resources to achieve a common outcome. GAO, *Results Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies,* GAO-06-15 (Washington, D.C.: Oct 21, 2005).

partners. FPS officials said that they use an informal process to manage the Council membership and have repeatedly reported that they actively seek to add members to expand state and local representation. Of the Council members identified by FPS, 21 of the 26 are federal agencies, 3 are state or local agencies, and 2 are non-governmental organizations. Officials from all 5 state and local government and non-governmental organizations told us that they were either unaware or did not consider themselves to be members of the Council. Furthermore, the Council currently has no representation from tribal and territorial governments. Having active representation from state, local, tribal, and territorial governments on the Council would be particularly helpful, given that FPS's interaction with the cross-sector councils that represent these perspectives has been limited or non-existent. As previously discussed, the SLTTGCC provides all 18 sectors a mechanism to coordinate with non-federal government organizations. According to the 2010 plan, the SLTTGCC had liaisons who were fully integrated into the Council. However, both SLTTGCC officials and FPS officials indicated that there has been limited interaction. During our review, FPS reached out to the SLTTGCC to discuss opportunities to increase partnering activities. FPS officials reported having never worked with the Regional Consortium Coordinating Council, which includes state and local government representatives. With limited representation on the Council and little or no interaction with certain cross-sector councils, the sector is missing opportunities to engage and integrate the experience, knowledge, and priorities of state, local, tribal and territorial partners into the plan to help ensure buy-in for protecting critical infrastructure across all levels of government.

Moreover, the Council has become progressively less active over the years. According to the 2011 annual report, the lead agency convenes Council meetings quarterly and communicates information about threats, incidents, and effective protection-related practices to sector partners. However, Council members indicated that the frequency of meetings has steadily declined over the years. In 2011, FPS held only one meeting in January; its next meeting was held in May 2012. No working groups or other activities occurred in the interim. At the 2011 meeting, there was a total of four non–DHS Council members who attended. FPS's May 2012 Council meeting may have reflected increased interest, with 14 agencies other than DHS in attendance. However, only one attendee represented state, local, tribal or territorial governments; all other attendees were from federal agencies. FPS officials acknowledged that participation of Council members has been decreasing every year. Most Council members representing federal agencies said that interaction with the sector had not

been helpful since their agencies actively participate in the ISC, which provides the guidance their agencies need to meet federal physical security standards. Nevertheless, some Council members said that the sector was valuable as a resource for coordinating security activities and potentially developing a uniform risk assessment tool. Since the sector covers a larger and broader set of government facilities than the ISC—such as military, state, local, tribal and territorial facilities—the potential benefits of collaboration, as discussed earlier, could lead to a more comprehensive approach to protecting critical government facilities.

FPS's Capacity to Lead the Sector Hindered by Its Fee Structure and Lack of Action Plan

FPS has identified its limited resources as a significant challenge to leading a sector as large and diverse as the government facilities sector. The 2010 plan states that the sector includes more than 900,000 federal assets, as well as assets from 56 states and territories; more than 3,000 counties; 17,000 local governments; and 564 federally recognized tribal nations. In addition, these facilities represent a wide variety of uses, both domestically and overseas, ranging from office buildings and courthouses to storage facilities and correctional facilities. FPS officials indicated that they have very limited staffing and no dedicated line of funding for activities related to leading the sector, and it was unclear if FPS's security fees could be used to cover the costs of serving as the lead agency for the sector. Because of limited resources, FPS officials said that they could only meet the NIPP's minimum reporting requirements and did not engage in other activities that could address the issues discussed earlier. For example, FPS officials said that they abandoned efforts related to strategic communications and marketing as described in the 2010 annual report, aimed at increasing awareness and participation across the sector because of resource constraints. FPS reported in 2010 that it did not have the capability to plan for any sector-specific agency investments. In 2011, FPS had less than one full-time equivalent employee engaged in sector-specific agency activities, which represents a decline from prior years when FPS had a full-time equivalent employee and several contract employees assisting with its sector responsibilities.

As discussed above, FPS is funded using a fee-based structure in which it collects funds from federal tenant agencies for security and protective services. We have previously reported that FPS's involvement in homeland security activities not directly related to facility protection is inconsistent with a requirement in the Homeland Security Act of 2002 that

FPS use funding from the fees it collects solely for the protection of federal government buildings and grounds.[19] We recommended to DHS that if FPS continues its involvement in activities not directly related to the protection of federal buildings and grounds, a funding process would be needed that is consistent with the requirement regarding the use of funds from agency rents and fees.

Notwithstanding issues related to how its fees may be used, FPS has not fully assessed the resource requirements for serving as the lead sector agency, because it has not completed an action plan or cost estimate for carrying out the 2010 plan. The 2010 plan states that determining the sector's priorities, program requirements, and funding needs for government facility protection is a sector objective. FPS previously reported it was developing an action plan to guide its implementation of the 2010 plan, but according to FPS officials, they are no longer pursuing this, because identifying steps FPS can and will take is difficult without knowing what funding or resources are available. FPS officials also told us that they originally estimated the cost of serving as the lead agency to be around $1 million, but did not provide us with the analysis to support this estimate.[20]

According to DHS officials, HSPD-7 is in the process of being updated to reassess how the NIPP and the sectors are overseeing the protection of critical infrastructure, which may result in the sector being restructured. For example, according to DHS, GSA, and Department of the Interior officials, GSA will become a co-lead agency, the monuments and icons sector will be subsumed within the government facilities sector, and an executive committee that includes the ISC may be formed to help advise the sector. Such changes may affect FPS's workload and resources as the lead agency.

An action plan could help FPS and DHS refocus efforts in the sector. We have recommended that agencies leading intergovernmental efforts use an action plan to establish priorities, provide rationale for resources, and

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

[20]According to FPS officials, half of the $1 million estimate was based on having three full-time equivalent staff and contractor support. The other half ($500,000) was based on travel costs for conferences, training, assessments, and to potentially engage subject matter expertise from the National Infrastructure Simulation and Analysis Center.

to propose strategies for addressing challenges.[21] An action plan could enable FPS and DHS to manage change by prioritizing the activities required of the sector's lead agency and identifying those activities that can be feasibly carried out by FPS given its current resource constraints. An action plan may also be useful to FPS for justifying additional resources, which may help address the challenge posed by its fee-based revenue structure.

Conclusions

FPS is responsible for leading efforts to identify, prioritize, and protect critical government facilities across all levels of government under the NIPP. The loss of critical government facilities and the people who work in them because of terrorism, natural hazards, or other causes could lead to catastrophic consequences. The lack of facility information, the absence of sector-wide risk assessments, and ineffective metrics and data undermine the implementation of a risk management approach as outlined by the NIPP risk management framework and envisioned in the 2010 plan. In addition, FPS has not effectively employed the NIPP sector partnership model to engage the Council and represent the depth, breadth, and interests of the sector, particularly non-federal partners. Consequently, key goals of the 2010 plan have not been met, and FPS is limited in its ability to productively contribute to the larger DHS effort to prioritize and safeguard the nation's most critical infrastructure. According to DHS officials, structural changes to the sector may already be under way. Yet, FPS and DHS do not have an informed understanding of the priorities and resources needed to fulfill the lead agency responsibilities, and structural changes may affect these priorities and available resources. An action plan could serve as a valuable tool for FPS and DHS to identify, in tandem with any structural changes, priorities that can be feasibly achieved and the associated resource requirements given FPS's fee-based revenue structure. This may, in turn, help address the overall limited progress made to date in the sector with implementing a risk management approach and developing effective partnerships.

[21]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).

Recommendation for Executive Action

To enhance the effectiveness of the government facilities sector, we recommend that the Secretary of DHS direct FPS, in partnership with IP and Council members, to develop and publish an action plan that identifies sector priorities and the resources required to carry out these priorities. With consideration of FPS's resource constraints, this plan should address FPS's limited progress with implementing a risk management approach and developing effective partnerships within the sector. The plan should address, at a minimum, steps needed to:

1. develop appropriate data on critical government facilities;
2. develop or coordinate a sector-wide risk assessment;
3. identify effective metrics and performance data to track progress toward the sector's strategic goals; and
4. increase the participation of and define the roles of non-federal Council members.

Agency Comments

We provided a draft report to DHS, GSA, Department of Education, Department of Health and Human Services, Department of State, National Archives and Records Administration, National Aeronautics and Space Administration, National Institute of Standards and Technology, Department of the Interior, Environmental Protection Agency, and Department of Justice. DHS concurred with our recommendation to develop and publish an action plan for the sector. DHS's full comments are reprinted in appendix II. The National Archives and Records Administration also agreed with our findings. DHS, GSA, and the National Institute of Standards and Technology provided technical comments, which we considered and incorporated, where appropriate. The other agencies did not provide comments on our draft report.

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

If you or your staffs have any questions on 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. Contact information and key contributors to the report are listed in appendix III.

Mark Goldstein
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

To assess the Federal Protective Service's (FPS) leadership of the government facilities sector, we reviewed Homeland Security Presidential Directive 7, Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP), and the 2010 Government Facilities Sector-Specific Plan (the 2010 plan). Based on these documents, we identified the implementation of a risk management approach and development of effective partnerships as two key activities of the NIPP and the 2010 plan that lead agencies are responsible for. These activities form the foundation for identifying, prioritizing, and protecting critical infrastructure. We reviewed the outcomes reported in the 2010 and 2011 sector annual reports to determine FPS's actions, and identified gaps between these actions and the goals and activities in the 2010 plan. We reviewed prior GAO reports and DHS Office of Inspector General reports on critical infrastructure to identify any challenges that FPS faces in leading the implementation of the 2010 plan and key practices on establishing performance metrics and interagency collaboration.

In addition, we interviewed FPS officials in Washington, D.C., about the 2010 plan, its sector-related activities as the lead agency, and any challenges to implementing the plan. We interviewed DHS officials from the Office of Infrastructure Protection and Interagency Security Committee about their role as sector partners and their interaction with FPS as the lead agency. We also interviewed members from the sector's Council about their role and participation in the Council and their interaction with FPS. We selected 16 of the 26 members of the Council based on several criteria, including their level of activity as determined by contributions to the 2010 plan and sector annual reports, or participation in the 2011 Council meeting, and all 5 of the state and local government members, and non-governmental organization members. Among federal members of the Council, we also selected federal agencies that served as the lead agencies for the monuments and icons sector, water sector, commercial facilities sector, and education subsector, and federal executive branch agencies with expertise in law enforcement or physical security applicable to the protection of government facilities.

Table 2: Council Member Agencies and Organizations Interviewed

Federal Agencies
Department of Homeland Security
Department of Education
Department of Health and Human Services
Department of State
National Archives and Records Administration
National Aeronautics and Space Administration
National Institute of Standards and Technology
Department of Interior
Environmental Protection Agency
Department of Justice
State and Local Government
City of Fort Worth, TX
City of Las Vegas, NV
New York State Division of Homeland Security and Emergency Preparedness
Non-Governmental Organizations
National Academy of Sciences
National Center for State Courts

Source: GAO.

We conducted this performance audit from December 2011 to 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.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

August 3, 2012

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

Re: Draft Report GAO-12-852, "CRITICAL INFRASTRUCTURE: DHS Needs to Refocus Its Efforts to Lead the Government Facilities Sector"

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 recognition of the challenges the National Protection and Programs Directorate's Federal Protective Service (FPS) faces as the designated Sector Specific Agency (SSA) for the Government Facilities Sector (GFS), particularly with regard to available resources to perform this role.

The National Infrastructure Protection Plan (NIPP) defines critical infrastructure protection and resilience roles and responsibilities, including the role and responsibilities of SSAs. Under the NIPP risk management framework, FPS is responsible for leading and coordinating six major elements sector-wide (i.e., set goals and objectives; identify assets, systems and networks; assess risks; prioritize infrastructure; implement protective programs; and measure effectiveness) to identify, prioritize, and measure progress towards protecting critical infrastructure. FPS is also responsible for establishing a risk management approach and developing effective partnerships for the sector, to include a wide variety of critical facilities and assets owned or leased at the federal, state, local, tribal, and territorial levels. As noted in this report, FPS has no dedicated line of funding for its activities as the lead agency for the sector, and faces both legal and resource constraints hindering its capacity to lead this large and diverse sector.

Independent of GAO's review, FPS has taken actions to enhance its coordination efforts as the sector-specific agency for the government facilities sector. These include establishing new relationships with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) to ensure broader state and local participation in sector coordination mechanisms. FPS is developing the resource estimates to perform this function and will include the requirements for consideration in future year budget requests.

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

Recommendation: Direct FPS, in partnership with IP and Council members, to develop and publish an action plan that identifies sector priorities and the resources required to carry out these priorities. With consideration of FPS's resource constraints, this plan should address FPS's limited progress with implementing a risk management approach and developing effective partnerships within the sector. The plan should address, at a minimum, steps needed to:

- Develop appropriate data on critical government facilities;
- Develop or coordinate a sector-wide risk assessment;
- Identify effective metrics or performance data to track progress towards the sector's strategic goals; and
- Increase the participation and define the roles of non-Federal Council members.

Response: Concur. FPS intends to engage with the GFS Government Coordinating Council, the Interagency Security Committee, and the SLTTGCC to identify and address cross-cutting issues for the GFS while capitalizing on existing partnerships and coordination mechanisms among stakeholders. This effort will include developing an action plan to address the following:

- Develop appropriate data on critical government facilities.
- Develop a risk assessment methodology that can be used for the sector.
- Develop metrics and performance data required to track progress towards the sector's strategic goals.
- Collaborate with the SLTTGCC to increase participation in the Government Coordinating Council and establish sector-specific roles of non-Federal Council members according to the NIPP framework.

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

2

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, David Sausville, Assistant Director; Friendly Vang-Johnson; Jennifer DuBord; Delwen Jones; Steven Putansu; and Kathleen Gilhooly made key contributions to this report.

Related GAO Products

Federal Facility Protection

Federal Protective Service: Better Data on Facility Jurisdictions Needed to Enhance Collaboration with State and Local Law Enforcement. GAO-12-434. Washington, D.C.: March 27, 2012.

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.

Homeland Security: Protecting Federal Facilities Remains a Challenge for the Department of Homeland Security's Federal Protective Service. GAO-11-813T. Washington, D.C.: July 13, 2011.

Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security. GAO-11-492. Washington, D.C.: May 20, 2011.

Homeland Security: Ongoing Challenges Impact the Federal Protective Service's Ability to Protect Federal Facilities. GAO-10-506T. Washington, D.C.: March 16, 2010.

Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection. GAO-10-142. Washington, D.C.: October 23, 2009.

Homeland Security: Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist. GAO-09-1047T. Washington, D.C.: September 23, 2009.

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.

Homeland Security: Preliminary Observations on the Federal Protective Service's Efforts to Protect Federal Property. GAO-08-476T. Washington, D.C.: February 8, 2008.

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.

Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices. GAO-05-49. Washington, D.C.: November 30, 2004.

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

Critical Infrastructure Protection

Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities. GAO-11-537R. Washington, D.C.: May 19, 2011.

Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened. GAO-10-772. Washington, D.C.: September 23, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.

The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report. GAO-09-654R. Washington, D.C.: June 26, 2009.

Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination. GAO-08-36. Washington, D.C.: October 31, 2007.

Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving. GAO-07-1075T. Washington, D.C.: July 12, 2007.

Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. GAO-07-706R. Washington, D.C.: July 10, 2007.

Critical Infrastructure: Challenges Remain in Protecting Key Sectors. GAO-07-626T. Washington, D.C.: March 20, 2007.

Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39. Washington, D.C.: October 16, 2006.

Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information. GAO-06-383. Washington, D.C.: April 17, 2006.