



Testimony

Before the Subcommittee on Oversight,
Management, and Accountability,
Committee on Homeland Security,
House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, September 22, 2022

FEDERAL PROTECTIVE SERVICE

Many Approved Security
Recommendations Were
Not Implemented and
Preliminary Work
Suggests Law
Enforcement Deployments
Have Increased

Statement of Catina B. Latham,
Acting Director, Physical Infrastructure

GAO Highlights

Highlights of [GAO-22-106177](#), a testimony before the Subcommittee on Oversight, Management, and Accountability, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Over one-million federal employees and visitors depend on FPS to provide security and protection at more than 9,000 facilities across the country. FPS assesses these facilities to identify security risks and then recommends security measures. In addition to this work, FPS provides law enforcement services on a short-term basis or in specific situations for individual agencies.

This testimony focuses on (1) stakeholders' views about FPS's facility assessments and the status of its security recommendations and (2) preliminary observations on FPS's law enforcement deployments. This statement is based on past work issued in June 2021 ([GAO-21-464](#)) as well as ongoing work on FPS's security recommendations and its move to DHS's Management Directorate in 2019.

For the 2021 report, GAO held discussion groups with stakeholders from 27 randomly selected FPS-protected facilities to obtain their views of FPS's risk assessments. In ongoing work, GAO analyzed FPS data on security recommendations made from fiscal years 2017 through 2021, data on law enforcement deployments in fiscal years 2020 and 2021, and staffing data for fiscal year 2021.

GAO previously recommended that FPS provide additional detail in its cost estimates for security measures. GAO is reviewing FPS's actions to address this recommendation. GAO will continue to assess these issues and make recommendations as appropriate.

View [GAO-22-106177](#). For more information, contact Catina B. Latham at (202) 512-2834 or lathamc@gao.gov.

FEDERAL PROTECTIVE SERVICE

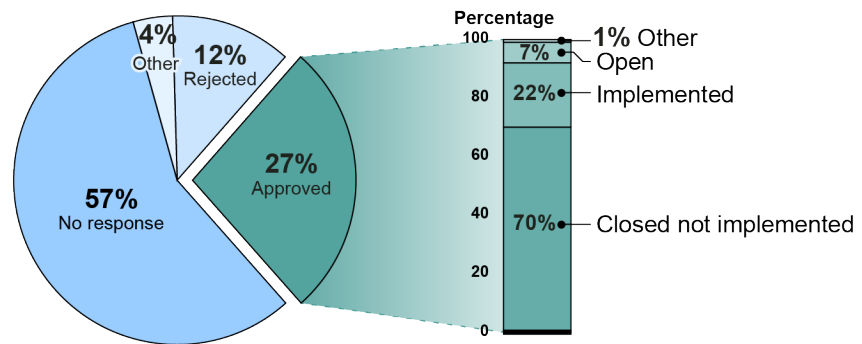
Many Approved Security Recommendations Were Not Implemented and Preliminary Work Suggests Law Enforcement Deployments Have Increased

What GAO Found

GAO reported in June 2021 that the Federal Protective Service's (FPS) stakeholders—tenant agency officials and building managers—held positive views about the content of FPS security assessment reports. In these reports, FPS made recommendations to address identified security vulnerabilities. Many of these stakeholders expressed concern that the cost estimates in the reports were not sufficiently detailed to inform their decisions on the recommendations.

In ongoing work, GAO found it was unclear if agencies were still in the process of deciding whether to approve most of FPS's recommendations or if they had accepted the security risks. FPS data also show an approval of a recommendation did not mean it would be implemented. For fiscal years 2017 through 2021, FPS made more than 25,000 security recommendations at nearly 5,000 facilities. FPS did not receive a response on whether agencies planned to implement over half of these recommendations. Of the recommendations approved for implementation, about 22 percent were implemented as of September 2022. GAO's ongoing work suggests recommendations were not implemented for reasons such as a lack of agency resources or tenant agency plans to move to a different facility.

Responses and Implementation Status of Approved Security Recommendations, Fiscal Years 2017–2021



Source: GAO analysis of data from FPS's Modified Infrastructure Survey Tool. | GAO-22-106177

Note: "Other" includes recommendations that FPS replaced with alternatives and recommendations that did not require an FSC response.

GAO's ongoing work also suggests that FPS has increased law enforcement officer deployments since fiscal year 2020. FPS has deployed law enforcement officers to augment its protection of federal facilities during protests and has an agreement to help another agency within the Department of Homeland Security to provide security at its facilities in the Southwest border region. GAO's ongoing work also found that FPS continues to face staffing shortages. At the end of fiscal year 2021, FPS had not filled 21 percent of its positions, including about 200 law enforcement positions. FPS officials cautioned that as facilities return to pre-COVID operations, these shortages could affect FPS's ability to carry out its responsibilities.

Chairman Correa, Ranking Member Meijer, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on security services provided by the Department of Homeland Security's (DHS) Federal Protective Service (FPS). FPS plays an important role in ensuring the day-to-day security of over one-million federal employees and visitors at more than 9,000 federal facilities. The General Services Administration (GSA) serves as the landlord for most of these facilities, with federal agencies renting space from GSA and thus serving as tenants. FPS provides security and protection at these facilities, in part, by conducting facility security assessments to identify security risks and recommending security measures for agencies to implement to address or mitigate these risks. Agencies' implementation of the recommended security measures is an important step in protecting employees, visitors, and facilities.

In addition to these efforts, FPS provides security as specific situations or events arise. This includes agreements to provide law enforcement on a short-term basis or in specific situations for individual agencies. For example, FPS has provided security at facilities in the Southwest border region for U.S. Customs and Border Protection and at locations of hurricane disasters for the Federal Emergency Management Agency.

We have designated federal real property management as a high-risk area since 2003, in part because of physical security challenges at federal facilities. One challenge we have identified in prior work has been FPS's ability to collaborate with GSA and tenant agencies—which we refer to as “stakeholders.”¹ My statement today focuses on:

- stakeholders' views on FPS's facility assessments and the implementation status of its security recommendations and
- preliminary observations on FPS's law enforcement deployments.

This statement is based in part on our report issued in June 2021 about stakeholders' perspectives on FPS's performance of key activities, including conducting facility security assessments. It is also based on our

¹We designated the broader area of federal real property management as a high-risk area due to the presence of unneeded and underutilized facilities, concerns with the reliability of real property data, and security challenges at federal facilities. GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021).

ongoing work related to FPS security recommendations and the impact of FPS's recent move to the Management Directorate within DHS.²

In conducting our prior work related to FPS's security assessments, we held six discussion groups with stakeholders from 27 randomly selected facilities where FPS provided services. The views of these stakeholder are not representative, but collectively provided insight into stakeholders' satisfaction with how FPS was performing key activities. We also compared FPS's facility security assessment reports to criteria in GAO's Cost Estimating and Assessment Guide.³ In our current work, we obtained data from FPS's risk assessment tool on recommendations made during fiscal years 2017 through 2021. We analyzed the data to identify the types of recommendations made and the approval and implementation status of the recommendations. We assessed the data against GAO data reliability standards, including reviewing FPS guidance and processes for safeguarding and checking the data for accuracy and completeness. We determined the data were sufficiently reliable for the purposes of describing the type and implementation status of FPS recommendations.

Our work to understand FPS's law enforcement deployments is ongoing. We analyzed data on the extent to which FPS law enforcement staff were deployed to support homeland security operations in fiscal year 2020 and fiscal year 2021 as well as data on the extent to which FPS had unstaffed positions as of the end of fiscal year 2021. Additionally, we interviewed officials from FPS, including five FPS Regional Directors, to understand how FPS's deployments and staff resources have changed since its move to the Management Directorate in 2019.⁴

We conducted this work 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

²GAO, *Federal Protective Service: Better Documented Cost Estimates Could Help Stakeholders Make Security Decisions*, [GAO-21-464](#) (Washington, D.C.: June 8, 2021).

³GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: March 2020).

⁴We selected Directors in the five largest regions in terms of FPS's authorized positions in fiscal year 2021.

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

Background

Organizational Responsibilities

FPS is responsible for the day-to-day protection of over a million people who work in or visit the over 9,000 federal facilities across the country held or leased by GSA. FPS provides both physical security and law enforcement services at these facilities.

- **Physical security activities.** FPS conducts facility security assessments and recommends security measures—such as security cameras, physical access control systems, and x-ray screening equipment. These measures are aimed at preventing security incidents. FPS also oversees Protective Security Officers (i.e., contract guards) who provide services such as screening visitors.⁵
- **Law enforcement activities.** FPS personnel respond to incidents, conduct criminal investigations, and can make arrests.

In addition to protecting GSA facilities, FPS participates in homeland security activities such as providing law enforcement, security, and emergency-response services during natural disasters and special events.⁶ In our January 2019 report and June 2019 testimony on FPS's organizational placement, we reported that FPS's responsibilities grew beyond solely protecting GSA facilities to include homeland security activities when it moved from GSA to DHS's Immigration and Customs Enforcement in March 2003.⁷ FPS continued to participate in such activities in each of its subsequent organizational placements in DHS: the National Protection and Programs Directorate (which was later re-

⁵For the purposes of this statement, we refer to Protective Security Officers as "contract guards."

⁶FPS derives its law enforcement authority with respect to the protection of buildings, grounds, and property that are owned, occupied, or secured by the Federal Government, and the persons on the property, from the Secretary of Homeland Security pursuant to 40 U.S.C. § 1315.

⁷FPS was transferred from GSA to DHS by the Homeland Security Act of 2002 (Pub. L. No. 107-296, § 403, 116 Stat. 2135, 2178) and placed within DHS's Bureau of Immigration and Customs Enforcement.

designated as the Cybersecurity and Infrastructure Security Agency)⁸ and the Management Directorate.⁹ FPS transitioned to DHS's Management Directorate—its current placement—in October 2019.¹⁰

Facility Security Assessments

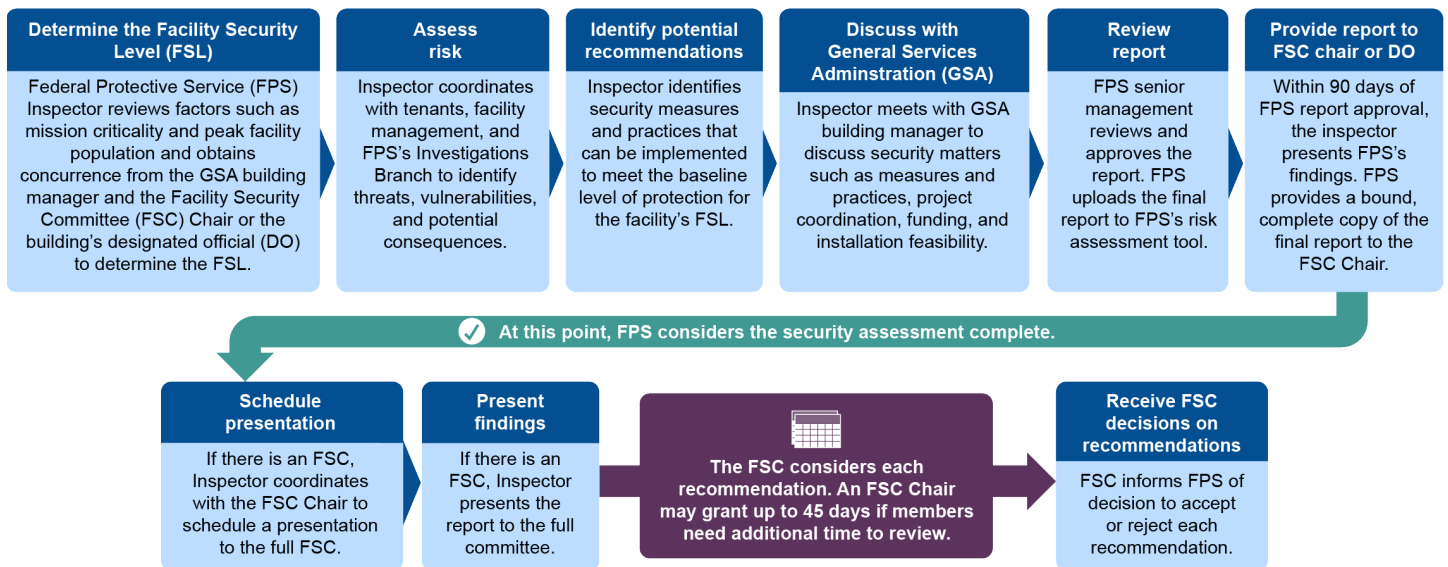
As part of FPS's physical security responsibilities, one of its key responsibilities is to conduct facility security assessments of federal facilities every 3 to 5 years to identify and evaluate potential risks (see fig. 1). As part of these assessments, FPS recommends security measures and practices to help prevent or mitigate these risks.

⁸The fiscal year 2010 DHS appropriations act transferred FPS from DHS's Immigration and Customs Enforcement to DHS's National Protection and Programs Directorate. Pub. L. No. 111-83, 123 Stat. 2142, 2156-57 (2009).

⁹In November 2018, when FPS was located in DHS's National Protection and Programs Directorate, the Cybersecurity and Infrastructure Security Agency Act of 2018 required DHS to determine the appropriate organizational placement for FPS. Pub. L. No. 115-278, § 2(a), 132 Stat. 4168. In May 2019, DHS announced its decision to transfer FPS to DHS's Management Directorate with FPS reporting to DHS's Undersecretary for Management. FPS transitioned to DHS's Management Directorate in October 2019.

¹⁰See also GAO, *Federal Protective Service's Organizational Placement: Considerations for Transition to the DHS Management Directorate*, [GAO-19-605T](#) (Washington, D.C.: June 11, 2019) and GAO, *Federal Protective Service: DHS Should Take Additional Steps to Evaluate Organizational Placement*, [GAO-19-122](#) (Washington, D.C.: Jan. 8, 2019).

Figure 1: Federal Protective Service’s (FPS) Process for Facility Security Assessments



Source: GAO analysis of FPS information. | GAO-22-106177

The Interagency Security Committee (ISC) and federal agencies that obtain space through GSA, known as tenant agencies, also have responsibilities associated with the facility security assessment process. ISC is a DHS-chaired organization that develops security standards for nonmilitary federal facilities in the United States. Among other things, ISC establishes standards that define the minimum physical security requirements and associated countermeasures. Under Executive Order 12977, FPS is required to follow ISC standards, including the ISC’s risk-management process standard, when conducting facility security assessments.¹¹

ISC standards require FPS to conduct these assessments every 3 to 5 years, depending on the security level of the facility.¹² FPS tracks

¹¹Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 19, 1995), as amended by Executive Order 13286, 68 Fed. Reg. 10619 (Mar. 5, 2003), requires executive branch departments and agencies to cooperate and comply with ISC’s policies and recommendations. See also, ISC, *The Risk Management Process: An Interagency Security Committee Standard*, 2021 Edition (2021).

¹²Facility security levels range from level I (lowest risk) to level V (highest risk) based on factors such as mission criticality and facility population. The security level designation determines the facility’s baseline security measures and practices.

scheduling and completion of its assessments for all facilities at all risk levels using data that the inspectors enter into FPS's risk assessment tool (i.e., Modified Infrastructure Survey Tool or MIST). FPS reported that in fiscal years 2017 through 2021 its inspectors completed 100 percent of facility security assessments for high-risk facilities within the required timeframe.¹³

ISC standards also specify that tenant agencies are responsible for making facility-specific security decisions, either as members of a Facility Security Committee (FSC) or through a designated official.¹⁴ An FSC is established for buildings occupied by multiple agencies and includes representatives from each of the tenant agencies. Members of the FSC or the designated official are responsible for making facility-specific security decisions. In multi-tenant facilities, the tenant agencies are responsible for funding most of the security measures proportionally based on the space they occupy in the facility.

ISC standards calls for the FSC to consider FPS's recommendations and decide whether to approve or disapprove (reject) the recommendations. The standard also states that the FSC may accept the risk of not implementing a security recommendation. The standard specifies that the FSC chair is to notify FPS of the decision within 45 days of receiving the assessment report. FPS records whether the FSC approved or rejected the recommendations from the facility security assessment into FPS's risk assessment tool. In addition, FPS records the results of the facility security assessments, including the identified vulnerabilities and the recommended security measures. If the FSC did not provide a decision to FPS within 45 days of receiving the FPS assessment and recommendation, FPS enters a status of "no response" into its risk assessment tool.

FPS Budget and Staff

FPS is entirely funded by the fees it charges agencies for its services and does not receive a direct appropriation from the general fund of the Treasury. For fiscal year 2021, FPS had an annual budget—based on revenue from the fees—of about \$1.6 billion. The rates FPS can charge agencies for basic security services must be approved by the Office of

¹³DHS, FY 2019–2021 *Annual Performance Report*, (Washington, D.C.: February 2020) and DHS, *Congressional Budget Justification for Fiscal Year 2023*, (Washington, D.C.: March 25, 2022).

¹⁴The federal agency with funding authority for security recommendations is the decision-maker for a single-tenant facility's security. Throughout this document, FSC is used to encompass both the FSC and the designated official.

Management and Budget. FPS also charges agencies fees for services beyond basic security.

In May 2021, FPS reported that it employed roughly 1,300 staff across 11 regional offices and headquarters. This workforce consists of law enforcement and non-law enforcement staff. Law enforcement staff include inspectors and criminal investigators. Law enforcement staff also include the Rapid Protection Force, which is a team that FPS can quickly deploy to heightened security situations. Non-law enforcement staff provide mission support. FPS also manages and oversees approximately 15,000 contract guards posted at federal facilities. The duties of contract guards include controlling access to facilities across the country; conducting screening at access points to prevent the entry of prohibited items, such as weapons and explosives; and responding to emergency situations involving facility safety and security.

Stakeholders Were Generally Satisfied with FPS's Security Assessment Process; Yet Many FPS Recommendations Were Not Implemented

Stakeholders Generally Held Positive Views of FPS's Security Assessment Process but Raised Concerns That Cost Estimates Lacked Important Details

In June 2021, we reported that the participants of our discussion groups—tenant agency officials and GSA building managers—generally held positive views about the content of FPS's security assessment reports and FPS's communication about the reports.¹⁵ Participants from all six- discussion groups characterized the reports as thorough, comprehensive, timely, and useful. Many participants also expressed satisfaction with FPS's communication of the security assessment results. However, several building manager participants told us that they had not been invited to an FPS presentation of security assessment results. According to the FPS *Facility Security Assessment Manual*, FPS is to work with the FSC chair to schedule and hold a presentation of the

¹⁵[GAO-21-464](#).

security assessment results to the committee. The FSC chair is responsible for inviting members of the committee to meetings.

However, we also reported that many stakeholders expressed concern with the cost estimates FPS provides in its security assessment reports.¹⁶ Participants from all three groups of building managers and one group of tenant agency participants said that FPS's cost estimates are not sufficiently detailed to inform participants' decisions on recommended security measures and practices.¹⁷ Based on the comments from our discussion group participants, stakeholders' concerns with cost estimates may discourage them from implementing security measures intended to reduce security risks. For example, one building manager participant observed that lack of details about cost estimates caused delays and resulted in unimplemented recommendations.

Given these concerns, we reviewed the most recent security assessment reports for the 27 buildings we selected. We found that selected FPS security assessment reports lacked documentation of important information that would help FSCs use the cost estimates to make decisions. According to ISC standards, FPS is required to provide a detailed description of work and cost estimates for each recommended security measure and practice.¹⁸ This requirement is reinforced by a 2018 memorandum of agreement with GSA in which FPS committed to provide cost estimates as part of its security assessment reports. In addition, according to GAO's Cost Estimating and Assessment Guide, cost estimates should provide information about the assumptions and sources used to develop an estimate so that decision-makers can understand the level of uncertainty around the estimate.

In our June 2021 report, we recommended that the Director of FPS ensure that Facility Security Assessment reports document the assumptions and sources used to develop the cost estimate for each recommended security measure.¹⁹ As of August 2022, FPS had taken steps to address our recommendation in part by updating its directive and

¹⁶[GAO-21-464](#).

¹⁷No participants commented positively about cost estimates in FPS's security assessment reports.

¹⁸ISC, *The Risk Management Process: An Interagency Security Committee Standard* 2021 Edition (2021).

¹⁹[GAO-21-464](#).

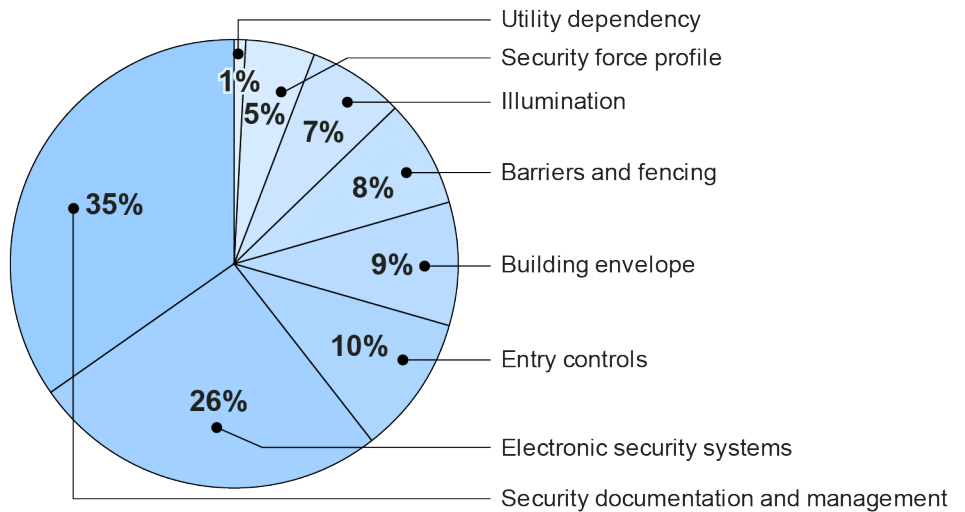
manual for conducting facility security assessments. We are assessing FPS's actions to determine if they fully address our recommendation.

FPS Data Indicate That Security Recommendations Are Generally Not Implemented

As previously discussed, FSCs are responsible for accepting a recommended security measure or rejecting it and thereby accepting the risk of not implementing it. Between fiscal years 2017 through 2021, FPS made more than 25,000 security recommendations at nearly 5,000 federal facilities. These recommendations ranged from addressing physical vulnerabilities to ensuring policy or guidance documents in the following categories (see fig. 2).

- **Barriers and fencing**—physical obstacles used to restrict access to facilities. Barriers are fixed or movable objects, such as bollards or spike systems, that are used to mitigate or reduce the impact of a vehicle ramming a building or a checkpoint.
- **Building envelope**—exterior surface of the building, including the doors, windows, façade, and roof.
- **Electronic security systems**—systems that are designed to prevent theft or intrusion and protect property and life, such as alarm systems and video surveillance systems.
- **Entry controls**—entry and access controls to the facility for employees, visitors, and vehicles, including locks, screening procedures, and parking security measures.
- **Illumination**—lighting of the facility, including entrances, fencing, and parking.
- **Security documentation and management**—documentation, policies, and procedures for the management of security threats and plans supporting security at the facility. Includes operational and emergency plans, as well as up-to-date security training.
- **Security force profile**—guards and guard services located at the facility.
- **Utility dependency**—the facility dependency on a utility service, such as electricity or water, and the presence of protective or emergency measures supporting provision of those services.

Figure 2: Federal Protective Service's (FPS) Recommendations by Vulnerability, Fiscal Years 2017–2021

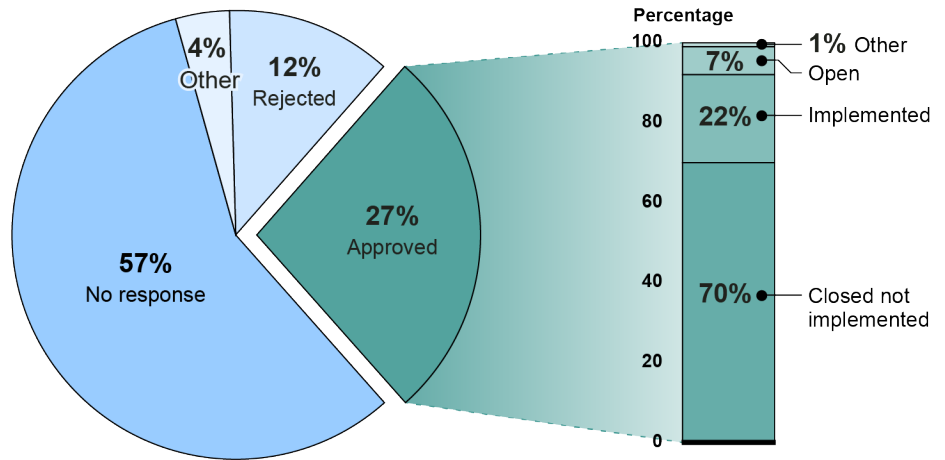


Source: GAO analysis of data from FPS's Modified Infrastructure Survey Tool. | GAO-22-106177

For the majority of FPS's recommendations, it was unclear from FPS's data if the FSC's were still in the process of deciding whether to approve the recommendations or had accepted the security risks. The data (discussed below) indicates that FPS did not receive notification of the FSCs' decisions to approve or reject more than half of the 25,000 security recommendations within 45 days of receiving the recommendation as called for in the ISC standard. As a result, FPS recorded the status of these recommendations as "no response," as noted earlier.

FPS data also show an FSC's approval of a recommendation does not necessarily mean it will be implemented. Of the 27 percent) of the recommendations approved by the FSCs, about 22 percent (about 1,500), were implemented as of September 2022 (see fig. 3).

Figure 3: Facility Security Committees' Responses and Implementation Status of Approved Security Recommendations, Fiscal Years 2017–2021



Source: GAO analysis of data from FPS's Modified Infrastructure Survey Tool. | GAO-22-106177

Note: "Other" includes recommendations that FPS replaced with alternatives and recommendations that did not require an FSC response.

Our preliminary findings from our ongoing work suggest a range of reasons for approved recommendations not being implemented. For example, FPS's data indicate that a recommendation may not be implemented for reasons such as a lack of agency resources to implement it or the tenant plans to move to a different facility. FPS officials also noted that some recommendations stay open for years because it can take time to secure the funding necessary to implement more costly security measures. Our ongoing work will identify factors that influence FSC decisions to approve or reject FPS security recommendations. We are also exploring what issues might be contributing to FPS not receiving a decision from the FSCs and contributing to approved recommendations not being implemented. We expect to report on this work in early 2023.

Our Preliminary Work Shows That FPS Has Increased Law Enforcement Deployments and Continues to Face Staffing Shortages

In addition to conducting facility security assessments, FPS provides law enforcement services. Our preliminary findings from our ongoing work show that FPS has increased its deployment of law enforcement officers since fiscal year 2020. FPS's deployments, for example, augment security at FPS-protected facilities or support other DHS components' homeland security operations, such as securing facilities at the nation's borders or disaster locations. In fiscal year 2021, for example, FPS deployed law enforcement officers to augment security at FPS-protected facilities during protests. As another example, in June 2022, FPS and DHS's U.S. Customs and Border Protection (CBP) signed an agreement to enable FPS to detail law enforcement officers to, among other things, provide security at CBP facilities, such as at migrant housing units, in the Southwest border region.²⁰ FPS's deployments in fiscal years 2020 and 2021 involved law enforcement officers from its Rapid Protection Force and other FPS law enforcement officers, most of whom are assigned to FPS regional offices and headquarters.²¹

FPS officials said that FPS is more involved in other DHS components' homeland security operations since the agency moved from the Cybersecurity and Infrastructure Security Agency to the Management Directorate in October 2019.²² They said FPS is more involved because the Acting Undersecretary for Management has shown support for FPS's facility protection mission and legal authorities, and ensured that DHS components are aware of FPS's role. FPS officials also said that their increased participation in homeland security operations has improved the

²⁰The law enforcement support FPS provides other federal agencies, and the fees FPS charges for this support, are governed by agreements between FPS and the other agencies.

²¹An FPS official involved in planning for deploying FPS law enforcement officers said that FPS sometimes uses contract guards to support homeland security operations. Contract guards check identification cards, perform basic patrol, and monitor camera systems.

²²In November 2018, when FPS was located in DHS's National Protection and Programs Directorate, the Cybersecurity and Infrastructure Security Agency Act of 2018 re-designated the National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency and required DHS to determine the appropriate organizational placement for FPS. See Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2(a), 132 Stat. 4168, 4184. In May 2019, DHS announced its decision to transfer FPS to DHS's Management Directorate with FPS reporting to DHS's Undersecretary for Management. FPS transitioned to DHS's Management Directorate in October 2019.

agency's credibility within DHS; they said this improved credibility has been one of the benefits of moving to the Management Directorate.

However, in the Management Directorate FPS has continued to face staffing shortages. In June 2010, when FPS was in the agency that was later re-designated as the Cybersecurity and Infrastructure Security Agency, we reported that FPS had difficulty obtaining the staffing needed to adequately protect federal facilities.²³ FPS's staffing difficulties have continued. At the end of fiscal year 2021, FPS reported that it had not filled 21 percent of its positions, including about 20 law enforcement positions in its Rapid Protection Force and about 180 additional law enforcement positions. However, two FPS Regional Directors we interviewed as part of our ongoing work said the current pandemic environment of limited occupancy in federal facilities has resulted in fewer incidents at facilities needing FPS's attention. The Directors cautioned that as facilities return to pre-COVID operations, FPS's staffing shortages could affect its ability to carry out its responsibilities.

We are currently conducting work on how deployments have changed since FPS's move to the Management Directorate and how FPS and the Management Directorate are addressing FPS's staffing shortages. We expect to issue a report on this work by the end of 2022.

Chairman Correa, Ranking Member Meijer, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Catina B. Latham, Acting Director, Physical Infrastructure, at (202) 512-2834 or LathamC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Maria Edelstein (Assistant Director); Sue Bernstein; Mallory Bryan; Roshni Davé; Geoffrey Hamilton; Alicia Loucks; John F. Miller; Josh Ormond; Steven Putansu; Anna Beth Smith; Janet Temko-Blinder; and Elizabeth Wood.

²³GAO, *Homeland Security: Preliminary Observations on the Federal Protective Service's Workforce Analysis and Planning Efforts*, [GAO-10-802R](#) (Washington, D.C.: June 14, 2010).

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

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

