United States Government Accountability Office

Testimony Before the Subcommittee on Economic Development, Public Buildings, and Emergency Management, Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, July 23, 2024

FEDERAL FACILITY SECURITY

Preliminary Results Show That Challenges Remain in Guard Performance and Oversight

Statement of David Marroni, Director, Physical Infrastructure Team

GAO-24-107599

GAO Highlights

Highlights of GAO-24-107599, a testimony before the Subcommittee on Economic Development, Public Buildings, and Emergency Management, Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

Federal real property has been on GAO's High-Risk List since 2003, in part due to threats to federal facilities. Past attacks on federal buildings demonstrate that the security of federal facilities remains a high-risk area. FPS, within the Department of Homeland Security, is responsible for protecting thousands of federal facilities. FPS employs contract guards at 2,500 federal facilities at a cost of almost $1.7 billion in fiscal year 2024.

This testimony discusses the preliminary results of an ongoing GAO review that focuses on (1) how effective FPS contract guards are at detecting prohibited items and FPS's efforts to improve detection, and (2) stakeholders' views on whether FPS data systems have improved oversight of the contract guard program.

To determine the effectiveness of FPS guards in detecting prohibited items, GAO conducted 27 covert tests at a nongeneralizable sample of 14 federal facilities and analyzed data from FPS's covert tests. To obtain stakeholders' views on FPS's data systems, GAO reviewed information on the systems and interviewed stakeholders, including FPS officials, federal tenants, guard unions, and security guard companies.

GAO provided a draft of this statement to FPS. FPS determined that some information was law enforcement sensitive. We withheld that information from this statement and incorporated other comments as appropriate. GAO plans to complete its work and issue a report on these issues by the end of the year.

View GAO-24-107599. For more information, contact David Marroni, Director, Physical Infrastructure, at (202) 512-2834 or MarroniD@gao.gov

July 23, 2024

FEDERAL FACILITY SECURITY

Preliminary Results Show That Challenges Remain in Guard Performance and Oversight

What GAO Found

To secure federal facilities and protect employees and visitors, the Federal Protective Service (FPS) manages and oversees more than 13,000 contract guards, whose duties include controlling facility access and screening visitors to detect prohibited items. To determine if FPS was effectively protecting federal facilities, GAO investigators conducted 27 covert tests at 14 selected federal buildings in early 2024. During these tests, GAO investigators had a prohibited item—a baton, pepper spray, or a multi-purpose tool with a knife—inside a bag that they attempted to bring into the building. FPS contract guards failed to detect prohibited items in about half of GAO's tests.

FPS conducts its own covert tests, the results of which were consistent with GAO's tests. While FPS determined that the specifics of its testing program are law enforcement sensitive, FPS officials said they have several reform efforts underway to improve contract guards' detection of prohibited items. Those efforts include (1) redesigning the initial training course for contract guards, (2) increasing on-the-job training, and (3) collecting covert testing data to identify common causes of covert test failures.

Stakeholders identified data system challenges that undermine FPS's productivity and oversight of contract guards. FPS developed data systems to improve oversight of the contract guard workforce in response to previous GAO recommendations. The Post Tracking System, initially piloted in 2018, was expected to be the system of record for ensuring that every post was staffed by a qualified guard for the correct time frames, but it has yet to be fully implemented in any region. In addition, stakeholders said the system continues to face technology, data reliability, and interoperability challenges and has not delivered the promised capabilities. This negatively affects the productivity of FPS's oversight efforts, according to stakeholders. Some FPS officials also said they do not use the reports for billing the government because the data are inaccurate or incomplete. Consequently, even in areas that have deployed the system, FPS continues to use an old paper-based system for billing and oversight tasks.

Chairman Perry, Ranking Member Titus, and Members of the Subcommittee:

Thank you for the opportunity to be here today to discuss our work on security at Federal Protective Service (FPS) facilities, in two areas: (1) detection of prohibited items by the guards who work under contract with FPS, and (2) FPS's oversight of Protective Security Officers (i.e., contract guards).[1] For 21 years, managing federal real property has remained on GAO's High-Risk List, in part due to threats to federal facilities.[2] Past attacks on federal facilities include the April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, in which 168 people died. More recent attacks—which were stopped by FPS contract guards—include a 2019 shooting at a Dallas federal facility, a 2021 shooting at a Social Security Administration facility, and an armed attempt to breach security at the Federal Bureau of Investigation's Cincinnati Field Office in 2022.

FPS is within the Department of Homeland Security (DHS) and is responsible for protecting about 9,000 federal facilities. FPS spent almost $1.7 billion on contract guards, which represented more than 76 percent of its budget, in fiscal year 2024. FPS officers and more than 13,000 contract guards control access to facilities, conduct access point screenings to detect prohibited items, and respond to safety and security emergencies.

In our past work, we identified several challenges to the security of federal buildings. In covert tests conducted in 2009, we carried components of improvised explosive devices into federal facilities, undetected by FPS guards. In 2010, we reported that in FPS's internal covert testing, FPS guards identified prohibited items in 18 of 53 tests. We found these security vulnerabilities were potentially caused by insufficient training for guards and FPS's failure to maintain a comprehensive system to ensure that guards were appropriately trained. Other challenges included staffing levels, human capital management, and inconsistent guidance about how and when guard inspections should

[1]For the purposes of this statement, we call Protective Security Officers "contract guards."

[2]The Managing Federal Real Property area was added to GAO's High-Risk List in 2003 and remained on the most recent update to the High-Risk list in 2023. See GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: Jan. 1, 2003) and *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

be performed. We have made a number of recommendations to FPS to help address these issues, some of which FPS has implemented.

Given the potential threats, it is imperative that FPS provides its more than 13,000 contract guards the training they need to secure federal facilities and protect employees and visitors. However, we have identified guard training and oversight weaknesses since 2008.[3]

My testimony today provides our preliminary observations from our ongoing review of security at federal facilities and FPS oversight of contract guards. My statement focuses on (1) how effective FPS contract guards are at detecting certain types of prohibited items at selected federal facilities and FPS's efforts to improve detection, and (2) stakeholders' views on whether FPS data systems have improved oversight of the contract guard program. In reviewing a draft of this statement, FPS determined that some information was law enforcement sensitive. We withheld that information from this statement. In the coming months, we plan to finalize our review and issue a final report, which may include a restricted version.

To determine how effectively FPS guards detected and excluded prohibited items from being brought into selected federal facilities, we conducted 27 covert tests by attempting to bring prohibited items (specifically, a knife, a baton, and pepper spray) into a nongeneralizable sample of 14 federal facilities.[4] The Interagency Security Committee Standard for determining facility security levels outlines several factors facility managers should use, including the facility's population and facility size. Facility security levels range from level 1 (lowest risk) to level 5

[3]GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Raise Concerns About Protection of Federal Facilities*, GAO-08-914T (Washington, D.C.: Jun. 18, 2008); GAO, *Federal Protective Service: Actions Needed to Assess Risk and Better Manage Contact Guards at Federal Facilities*, GAO-12-739 (Washington, D.C.: Aug. 10, 2012); GAO, *Federal Protective Service: More Collaboration on Hiring and Additional Performance Information Needed*, GAO-23-105361 (Washington, D.C.: Dec. 15, 2022); GAO, *Federal Facilities: Continued Oversight of Security Recommendations Needed*, GAO-24-107137 (Washington, D.C.: Nov. 29, 2023).

[4]Prohibited items used in the covert tests met the specifications of prohibited items listed in the following federal standard, Interagency Security Committee, *Items Prohibited in Federal Facilities, An Interagency Security Committee Standard*, (Washington, D.C.: 2022). In some cases, we conducted multiple tests at the same facility, which means that the number of tests is larger than the number of facilities tested. We conducted multiple tests in all high-risk facilities, and in one low-risk facility, to test the ability of contract guards to detect different types of prohibited items. We attempted to smuggle one type of prohibited item during each test.

(highest risk).[5] These facilities had varying levels of security and screening procedures, in part because of their security level. We selected these federal facilities based on several factors, including public access, location, size, and the number of federal tenants in the facilities.

We also analyzed FPS data from fiscal years 2020 to 2023 about the outcomes of FPS internal covert tests. We assessed the reliability of the data by reviewing FPS guidance and processes for safeguarding and checking the data for accuracy and completeness. When we found discrepancies such as missing data or data entry errors, we brought them to FPS's attention and worked with FPS to correct the discrepancies before conducting our analyses.

To collect stakeholders' views on whether FPS data systems have helped address challenges with overseeing the contract guard program, we interviewed FPS officials, federal tenant agencies, unions, and security guard companies about system capabilities that support contract guard oversight. We also observed the operation of the systems and reviewed agency policies and guidance related to oversight efforts. Specifically, we reviewed FPS guidance and documentation on several data systems to determine their purpose and the information used by agency officials.

The ongoing work on which this statement is based is being conducted 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 conducted our related investigative work in accordance with investigation standards prescribed by the Council of the Inspectors General on Integrity and

[5]Interagency Security Committee, *The Risk Management Process: An Interagency Security Committee Standard*, (Washington, D.C.: 2021). The Interagency Security Committee (ISC), housed within DHS's Cybersecurity and Infrastructure Security Agency, is responsible for developing federal security policies and standards to enhance the quality and effectiveness of security in, and protection of, civilian federal facilities. The ISC was established in 1995 under Executive Order 12977 to enhance the quality and effectiveness of security in and protection of federal facilities in the United States occupied by federal employees for nonmilitary activities. Executive Order 12977, *Interagency Security Committee*, 60 Fed. Reg. 54411 (Oct. 19, 1995), as amended by Executive Order 13286, *Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security*,68 Fed. Reg. 10619 (March 5, 2003). Executive Order 14111, *Interagency Security Committee*, issued in November 2023 supersedes Executive Order 12977. Executive Order 14111, 88 Fed. Reg. 83809 (Nov. 27, 2023)

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

Background

FPS Responsibilities

FPS conducts physical security, law enforcement, and contract guard oversight activities at federal facilities across the country, a majority of which are under the custody or control of the General Services Administration (GSA).[6]

- **Physical security activities.** FPS develops individual facility security assessments to identify and assess threats to and vulnerabilities for about 9,000 facilities. FPS then recommends appropriate countermeasures, such as security equipment, to address those threats and vulnerabilities.[7]
- **Law enforcement activities**. FPS's law enforcement activities include patrolling facilities, responding to incidents, conducting criminal investigations, and making arrests.[8]

  Contract guard oversight. FPS manages and oversees contract guards for various federal agencies at roughly 2,500 of the overall facilities it protects.[9] In its oversight role, FPS monitors vendor-provided training, manages the contracts of vendors who provide contract guards, and conducts other oversight activities, such as post visits and post inspections. For example, FPS officials review the operational readiness of contract guards at posts by conducting post visits, during which they evaluate the contract guard's knowledge of post orders and operational readiness requirements.

[6]FPS is funded through fees it charges agencies for its services and does not receive a direct appropriation from the general fund of the Treasury.

[7]In 2023, we recommended the Department Homeland Security improve its oversight ability to assess countermeasure implementation; GAO, *Federal Facilities: Improved Oversight Needed for Security Recommendations*, GAO-23-105649 (Washington, D.C.: May 8, 2023).

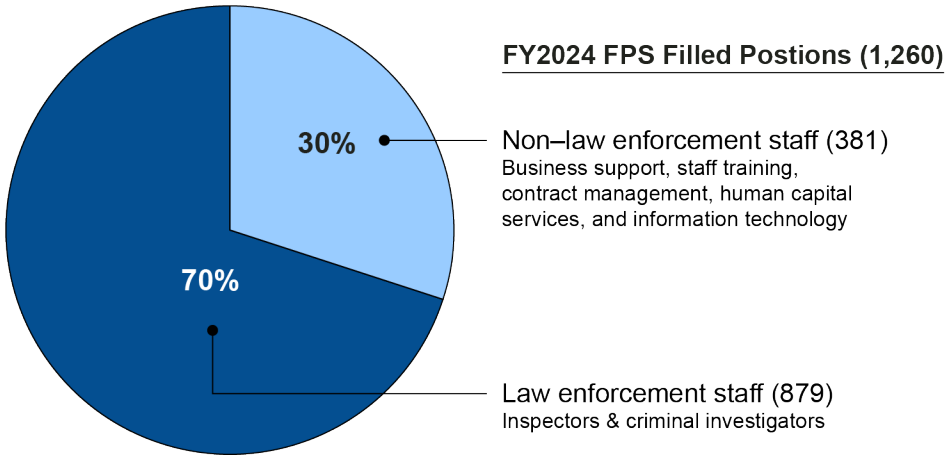
[8]GAO-23-105361.

[9]FPS charges federal agencies additional fees for agency and building specific services beyond basic security, such as contract guards and security patrols.

Staffing

In fiscal year 2024, FPS employed about 1,260 staff across 11 regional offices and headquarters.[10] The FPS workforce consists of law enforcement and non-law enforcement staff (see fig. 1).

Figure 1: Federal Protective Service Law Enforcement and Non-Law Enforcement Staff



Source: GAO analysis of FPS data. | GAO-24-107599

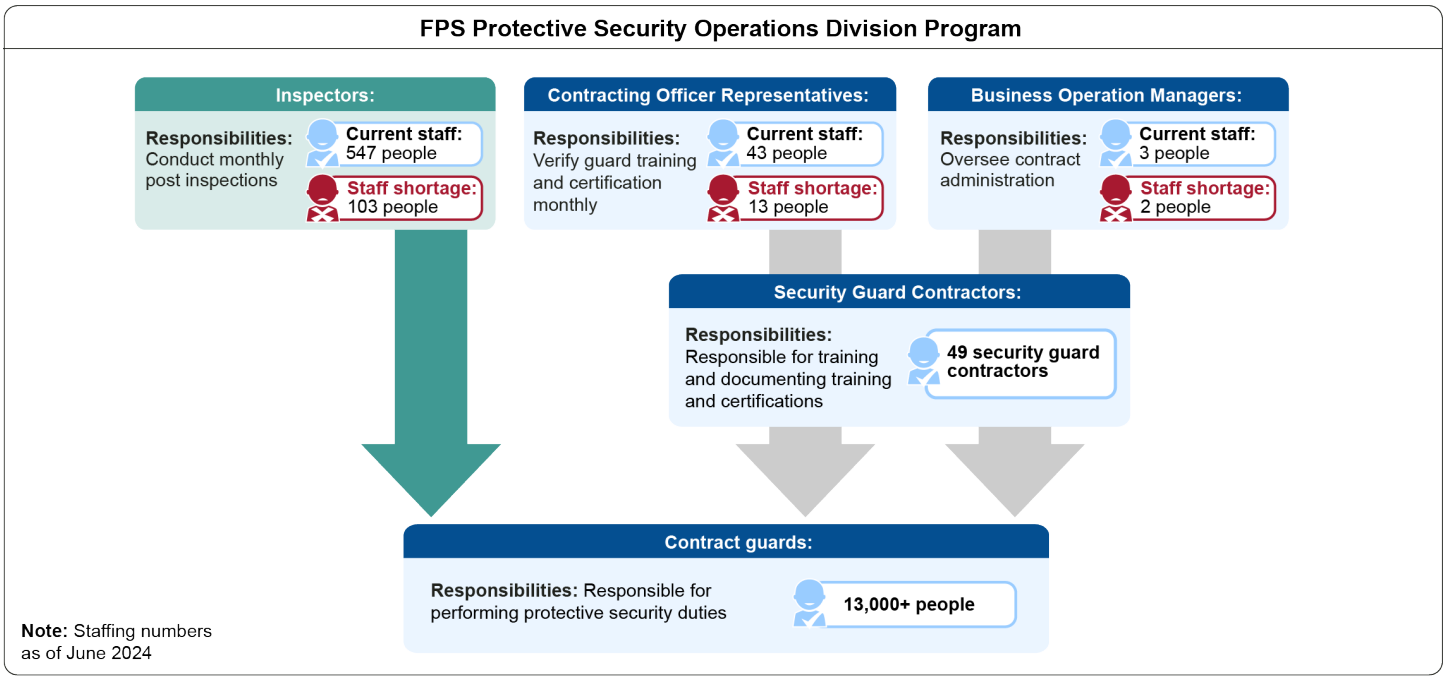
Law enforcement staff include inspectors and criminal investigators. Non-law enforcement staff provide business support such as staff training, contract management, human capital services, and information technology.[11] Both types of FPS staff provide oversight to over 13,000 contract guards.

The FPS Protective Security Operations Division is responsible for contract guard oversight. Figure 2 depicts staffing shortages among personnel who provide oversight to contract guards.

[10]For fiscal year 2024, FPS was authorized for 1,692 positions, according to FPS officials.

[11]GAO-23-105361.

Figure 2: Selected FPS Protective Security Operations Division Program Staffing



Source: GAO analysis of FPS information, GAO (icons). | GAO-24-107599

Note: FPS officials said additional headquarters and regional officials also play a role in providing oversight of the contract guard workforce but are not depicted in the above graphic.

FPS Inspectors, Contracting Officer Representatives (COR), and Business Operation Managers (BOM) are responsible for managing contract guards. Inspectors conduct monthly post inspections, Contracting Officer Representatives verify guard training and certification monthly, and Business Operation Managers oversee contract administration.[12] Contract guard vendors are responsible for training and documenting training and certifications in FPS systems.

In 2022, we reported FPS employed roughly 1,300 staff for fiscal year 2021, which reflected a staffing shortage of 21 percent.[13] FPS has 409 vacant positions, as of July 2024.

[12]Business Operation Managers provide oversight and monitoring over COR programs for FPS regions including budget, financial planning, revenue management, and acquisition.

[13]GAO-23-105361.

Contract Guard Responsibilities

Approximately 13,000 contract guards control access to about 2,500 federal facilities. Contract guards' responsibilities include screening at access points to prevent the entry of prohibited items, such as weapons and explosives, and responding to emergencies involving facility safety and security.

Prohibited Items

The Interagency Security Committee, of which FPS is a member, issued the *Items Prohibited in Federal Facilities, An Interagency Security Committee Standard*, which establishes a baseline list of prohibited items that includes firearms, dangerous weapons, or explosives because those items are designed, redesigned, used, intended for use, or readily converted to cause injury, death, or property damage. The Interagency Security Committee's *Items Prohibited in Federal Facilities* Standard notes that prohibited items also include any item banned by any applicable federal, state, local, or tribal ordinance. According to this standard, the list of prohibited items applies to all facility occupants, contractors, and visitors.

In some cases, the list of prohibited items is broader than what is legal to carry in the locations where federal facilities are located. For example, carrying pepper spray for self-defense purposes or pocketknives with a blade over certain lengths might be otherwise legal within a particular jurisdiction, but they are on the Interagency Security Committee's baseline list of items generally prohibited inside federal facilities. According to FPS officials, if an individual attempts to enter a federal facility with a prohibited yet otherwise legal item, the individual must remove the item from the property. Contract guards are authorized to detain individuals who refuse to comply with the contract guard's request to remove the item, according to FPS. FPS officials said that if an individual attempts to enter a federal facility with an illegal item, contract guards are authorized to seize the item; it is up to FPS personnel to issue a citation or arrest the individual if necessary.

Data Systems

We have found longstanding challenges with the data systems FPS uses to oversee contract guards.

- In 2009, we reported that FPS was using the Contracting Guard Employment Requirements Tracking System to monitor and verify contract guard training and certifications. However, the system was

not fully reliable.[14] This system was replaced later that year by the Risk Assessment and Management Program (RAMP).[15]

- In 2010, we recommended that FPS verify the accuracy of guard certification and training data in RAMP.[16]
- In 2012, we reported that RAMP, which was expected to improve FPS employees' administrative worktime efficiency, was no longer used after 3 years due to system issues.[17] FPS replaced this system with an interim vulnerability assessment tool, the Modified Infrastructure Survey Tool. This tool enabled FPS to conduct facility security assessments, but the program did not allow for oversight of the contract guard program. We recommended FPS address the Modified Infrastructure Survey Tool's limitations and develop and implement a new comprehensive and reliable system for contract guard oversight.[18]
- In 2014, we found that FPS continued to lack a comprehensive and reliable contract guard management system.[19]

As part of its efforts to address two of our recommendations from these reports, FPS developed two separate data systems to conduct contract guard oversight: the Post Tracking System and the Training and Academy Management System. FPS also developed PostNow to provide post data for contract guards. See table 1 for information on selected FPS data systems.

[14]GAO, *Homeland Security: Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered By Weaknesses in Its Contract Security Guard Program*, GAO-09-859T (Washington, D.C.: Jul. 8, 2009).

[15]GAO-12-739.

[16]GAO, *Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contact Guards,* GAO-10-341 (Washington, D.C.: Apr. 13, 2010).

[17]GAO-12-739.

[18]GAO-12-739.

[19]GAO, *Federal Protective Service: Protecting Federal Facilities Remains a Challenge*, GAO-14-623T (Washington, D.C.: May 21, 2014).

Table 1: Selected Federal Protective Service (FPS) Data Systems

Data System	System Users	System Purpose	Implementation Time Frame
The Post Tracking System	Contract guard vendors, FPS employees	Verifies individual contract guard identities and requisite qualifications to staff for a specific post	FPS expects all security contractors to be using the system in accordance with contractual terms by the end of fiscal year 2024
PostNow	FPS employees	Provides post data including type of post, type of security required, and assigned Contracting Officer Representative	Fully implemented
The Training and Academy Management System	Contract guard vendors, FPS employees	Tracks and maintains documentation for all required contract guard training and certifications	FPS expects this system to be fully implemented by calendar year 2025

Source: GAO analysis of FPS information. | GAO-24-107599

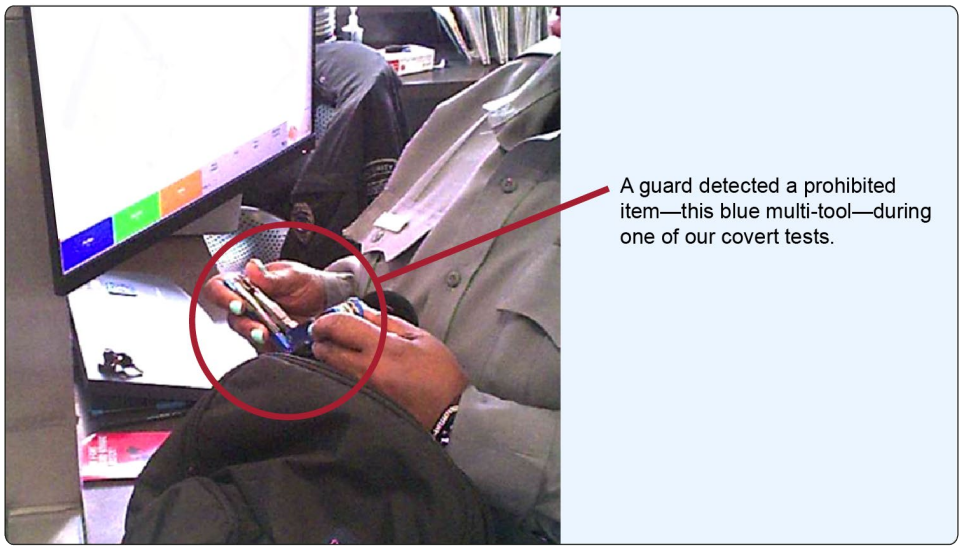
Contract Guards Regularly Failed Covert Tests at Selected Facilities, but FPS Has Efforts Underway to Improve the Detection of Prohibited Items

Contract Guards Did Not Detect Prohibited Items about Half the Time in Covert Tests

Our covert testing. In 13 of the 27 tests we conducted at selected locations, FPS contract guards did not detect the prohibited items we were attempting to smuggle into the facility. During our covert tests, our investigators had a prohibited item—specifically, a knife, a baton, or pepper spray—inside of a bag that they were bringing into the facility.[20] See figure 3 for a photo of a contract guard who successfully detected one of those prohibited items.

[20]Prohibited items used in the covert tests met the specifications of prohibited items listed in the following federal standard, Interagency Security Committee, *Items Prohibited in Federal Facilities, An Interagency Security Committee Standard* (Washington, D.C.: 2022). We packed each prohibited item in a backpack.

Figure 3: Contract Guard Detecting a Prohibited Item During GAO's Covert Testing



Source: GAO (photo). | GAO-24-107599

FPS Has Several Efforts Underway to Improve Detection of Prohibited Items

FPS has several reform efforts underway to improve contract guards' detection of prohibited items. These efforts include (1) redesigning the initial training course for contract guards, (2) adding more frequent opportunities for on-the-job training, and (3) collecting information about common causes of covert test failures.

Redesigning the initial training course for contract guards. FPS is in the process of redesigning its National Weapons Detection Training Program (NWDTP) course, according to an FPS official. The NWDTP is a 16-hour course that trains guards how to screen individuals at facility entrances and how to use tools—such as X-ray machines and metal detectors—to detect prohibited items. According to an FPS official, during the redesign process they reviewed industry standards, academic research about guards' use of screening tools, and leading screening practices that other federal agencies and the private sector have implemented. An FPS official said they plan to incorporate what they have learned into the updated course to ensure that guards are receiving the training they need to effectively detect prohibited items. According to an FPS official, they expect the updated course to be piloted by the end of fiscal year 2025.

Adding more frequent opportunities for on-the-job training. To supplement the NWDTP training, FPS developed an on-the-job training program to provide contract guards with more frequent learning opportunities. In 2023, FPS added a requirement for inspectors to conduct an on-the-job training at every screening post at least once annually. In addition, vendors must provide 2 hours of on-the-job training every 60 days for all contract guards who work at screening posts.

According to officials, FPS designed on-the-job trainings to reinforce NWDTP strategies and to provide contract guards with regular practice detecting prohibited items. FPS presents these trainings as learning opportunities; they are not covert tests. The on-the-job training kit includes several items that can be used in various training scenarios, such as a non-functioning firearm, a knife with a blade that is longer than 3 inches, and an inert pipe bomb. Inspectors use the items in the kit to evaluate guards' ability to accurately detect specific prohibited items, and to provide feedback if the guard has difficulty identifying the item. FPS is evaluating the effectiveness of its on-the-job training program and plans to use those findings to improve the program.

Collecting covert testing data. FPS also regularly conducts covert testing to evaluate contract guards' ability to detect prohibited items. FPS's testing results were consistent with our results. However, FPS determined that the specifics of the tests were law enforcement sensitive.

FPS currently compiles an internal covert testing database that houses information about the results of internal covert tests, causes for failures, and the types of remediation required when guards fail covert tests. However, based on our preliminary analysis, information in the database is inconsistent or insufficient in the following areas: data entry, information provided about root causes of failures, and information provided about remedial training for contract guards.

- **Data entry.** In our preliminary analysis of FPS data, we found that FPS staff enter covert test data inconsistently. For example, similar outcomes of similar tests are recorded differently (some appear as "pass" and some as "fail"), narrative descriptions have inconsistent levels of detail, and labels for test scenarios do not always match the narrative descriptions. FPS agreed that additional data quality checks could catch data entry errors and improve the accuracy of the data in the dataset. In addition, FPS acknowledged that providing consistent levels of detail in the narrative descriptions would help FPS staff

better determine the root causes for failures and appropriate corrective actions to address those failures.

- **Root cause.** According to our preliminary analysis of FPS data, the most common cause FPS listed in the dataset provides insufficient information about the root cause of a failure to detect a prohibited item. Specifically, when contract guards fail covert tests, FPS listed "human factor" as the cause more than 80 percent of the time.[21] When "human factor" is listed as the cause, we found multiple instances when the narrative description indicated the cause could be more accurately described as being due to the following: equipment issues, guards' failure to conduct secondary screenings properly, guards' failure to notify officials after detecting prohibited items, or other factors. According to FPS officials, "human factor" is too broad to identify the root cause of the failure or proactive steps that could prevent similar failures in the future. FPS acknowledged that updating the term "human factor" could provide more specific information about the cause of the failure. However, according to FPS, it will take time and additional resources to update the dataset.
- **Remedial training.** In our preliminary analysis of FPS data, we found that vendors assigned remedial training for similar failures inconsistently, in part because the root cause of the failure is not clearly identified in the dataset. For example, the types of assigned remedial training—and the duration of that training—varied when guards failed to detect improvised explosive devices during FPS covert tests. Some guards received explosive detection remedial training that was clearly aligned with the failure, some received unrelated training that focused on screening sensitive areas of the body, and some were required to retake the entire NWDTP course, only part of which is directly related to detection of improvised explosive devices. In explaining the variation, FPS officials told us that they do not dictate the type of remedial training that vendors should provide. Instead, FPS allows vendors to determine what type of training they will provide for their guards.

Our forthcoming report will further address these issues.

[21]Although "human factor" is the most common cause, three other causes appear in the data set: "training/process/technique" (15 percent), "equipment" (1 percent), and policy/post orders (0.4 percent).

Stakeholders Identified Data Systems Challenges That Undermine FPS's Productivity and Oversight of Contract Guards

In response to our prior recommendations, FPS developed two systems to oversee its contract guard workforce.[22] We previously recommended that FPS develop and implement a comprehensive and reliable system to provide oversight and verify that contract guards are current on all training and certification requirements.[23] We reported in April 2023, that the Post Tracking System and the Training and Academy Management System were neither completely implemented nor interoperable.[24] According to FPS officials we interviewed, the two systems FPS developed are unable to communicate with each other and have data reliability and technology challenges. In some cases, agency, union, and security guard contractors said these systems have not delivered promised capabilities and negatively affect the productivity of FPS's oversight efforts. Our forthcoming report will further address these issues.

Post Tracking System (PTS)

Under development since 2013 and initially piloted in 2018, PTS was expected to be the system of record for ensuring that every post was staffed by a qualified guard for the correct time frames in every FPS-protected facility.[25] More specifically, PTS was to facilitate signing in and out of the guard post, remotely verify that guard posts are staffed as required, and track guard certifications to ensure that qualified and cleared guards staff FPS posts. PTS was also expected to verify billing for guard contracts and report prohibited items that are detected. PTS was intended to interface with other agency systems (see fig. 4).

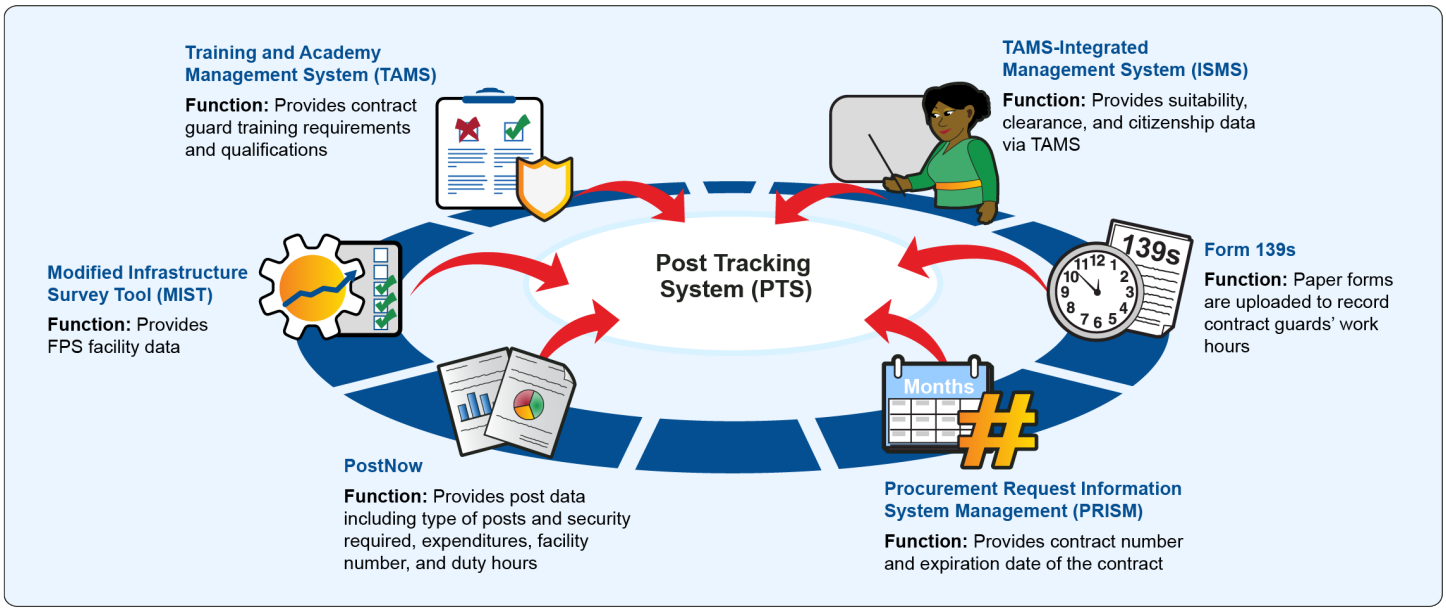
[22]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[23]GAO, *Federal Protective Service: Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities*, GAO-12-739 (Washington, D.C.: Aug. 10, 2012).

[24]GAO-23-106203.

[25]FPS defines a post as a defined security function (e.g., X-ray, magnetometer, Wand) for a guarded location.

Figure 4: Federal Protective Service (FPS) Systems That Inform the Post Tracking System



Source: GAO analysis of FPS information, GAO (icons). | GAO-24-107599

The nationwide deployment of PTS is ongoing; however, the system is not fully functional in any region because of technology, data reliability, and interoperability issues identified by FPS and security guard contractor officials. According to FPS data, 61 security guard contracts require deployment of PTS. FPS plans to add these requirements to additional contracts by the end of fiscal year 2024. However, PTS usage by regions and contractors varies, and PTS is not the system of record for any guard contract according to FPS officials. More specifically, some FPS regional officials said PTS utilization is never higher than 60 percent and can fall as low as 20 percent systemwide due to functional challenges. In April and May of 2024, FPS reported average daily utilization percentages for guards standing post per contract ranging from zero to 95 percent for 61 contracts. Of those 61 contracts, FPS reported most contracts had utilization percentages less than 75 percent.[26] Consequently, even in areas that have deployed PTS, FPS continues to require use of its old paper-based system for billing and guard verification.

[26]FPS data provided covered the week ending on May 26, 2024.

FPS and security guard contractor officials identified several challenges that continue to prevent PTS' successful deployment:

- **PTS interoperability.** According to the PTS Manual, the system is populated with data from five systems with information on training, security clearances, facilities, post responsibilities from contracts, and contractor information.[27] However, an FPS official said PTS does not have full automated interoperability, requiring FPS staff to manually upload data from each of the five systems. Several regional FPS officials and security guard contractors said this effort causes delays and extra administrative work. Furthermore, officials noted that because PTS relies on manual uploading data, PTS is not operating with the real-time data needed to inform FPS officials whether contract guards are qualified to stand post. In addition, several FPS officials said that PTS is not a user-friendly system for exporting the information needed to support oversight capabilities. Contract guards can enter detected prohibited item reports in PTS; however, the information cannot be exported to other FPS systems. These reports are required weekly from each FPS region. One FPS official told us that it takes 2 to 3 days each week to meet the requirement because the reports must be manually entered into another FPS system.
- **PTS technology issues.** FPS officials told us that security guard contractors routinely inform them that PTS does not allow qualified guards to sign into the system due to technology issues with guard identification cards, vendor-supplied equipment, or Internet connection problems. Security guard contractors said that their guards become frustrated by the myriad of problems and give up on using the system. There is an FPS Help Desk to help with tech issues; however, FPS officials said that PTS is used infrequently and continues to require security guard contractors to complete paper forms to document guard posts and work hours as an ongoing workaround.

  When multiple posts exist in one facility, FPS may set up a single post where contract guards sign in using PTS. However, according to a security guard contractor, the system sometimes crashes or stops working when multiple contract guards sign in or out around the same time. For example, one security guard contractor official said it is

[27]The five systems are the Training and Academy Management System, Integrated Security Management System, Modified Infrastructure Survey, PostNow, and the Procurement Request Information System Management. In previous PTS manuals, PostNow was referred to as PostX. Federal Protective Service. *Federal Protective Service Post Tracking System, User Manual for Administrator Contracting Officer Representatives (COR)*, Version 3.5. (Washington, D.C. Dec. 28, 2023).

common for multiple contract guards to stand in line waiting to sign in or out creating a long delay during shift changes. Furthermore, the company official said that if the contract guard cannot sign out by the time their shift ends, the company pays overtime; an additional cost the company did not anticipate.

- **PTS data reliability.** FPS officials we interviewed identified numerous errors in PTS's underlying data, such as inaccurate descriptions of post requirements. Also, officials said the manual upload of data from multiple data systems into PTS can cause errors. For example, FPS is manually uploading information into PTS from another FPS system, PostNow, to indicate which posts need guard coverage and to outline the required guard qualifications for each post.[28] However, several FPS regional officials told us that due to a lack of guidance or standards, the aggregated information causes errors once uploaded to PTS. FPS officials said these errors can incorrectly flag contract guards as not qualified to stand post. Furthermore, this information must then be corrected by FPS officials, which is a time-consuming process.

  Several FPS guard contractors we interviewed said they could not use PTS to document contract guards' time and attendance because the data are unreliable—too often they cannot connect to the server, or the system will not allow a contract guard to sign in due to a technical issue. A Help Desk provides support for technical issues, but all the security guard contractors we interviewed said they instead rely on the legacy paper process and their own company software to track time and attendance for contract guards. Furthermore, some FPS officials we interviewed said they do not use the reports from PTS because the data are inaccurate or incomplete for billing verification. According to security guard contractors we interviewed, FPS has not requested security guard contractors' feedback on deficiencies or evaluated deficiencies within the system. These officials said they continue to spend valuable time and resources troubleshooting technology issues. Two guard contractors said that they needed to assign additional IT specialists to exclusively troubleshoot PTS issues, further increasing costs for a system that they have no plans to use as the system of record.

[28]PostNow is a system that provides information on FPS contract guard posts, responsibilities, type of security required, expenditures, facility number, and duty hours. It was initially developed as a stand-alone financial system to track expenses by post and was not intended to be used for other FPS databases.

Due to the technology issues discussed in this section, FPS officials told us that PTS has not yet delivered on promised capabilities. According to the PTS Vendor Guide, the system should automate oversight of contract guards, including automatically and remotely monitoring guard posts in real time to ensure that the post is staffed as required by qualified and cleared guards.[29] However, officials told us that PTS cannot remotely verify that guard posts are staffed based on real-time data. Tenant agency officials that have FPS contract guards protecting their facilities said that real-time information could inform FPS, security guard contractors, and tenant agencies. This in turn would allow them to reallocate resources to address a shortage of contract guards in specific locations.

For example, officials from two tenant agencies—Internal Revenue Service (IRS) and Social Security Administration (SSA)—expressed frustration with the lack of contract guards available to stand post at federal facilities.

- IRS officials said that they do not receive timely communication about how guard shortages affect their facilities, often learning weeks later that posts were not staffed from local IRS agency officials. IRS officials said these guard shortages have caused problems, security vulnerabilities, employee delays, and increased traffic due to closed entrances. Since fiscal year 2022, IRS officials reported they closed 30 Taxpayer Assistance Centers for a full day because of the lack of contract guards. IRS officials said that real-time information on post staffing and better communication would have allowed them to take proactive steps to limit such problems.
- SSA officials also said that FPS has been unable to provide a sufficient number of contract guards in the last 3 fiscal years, resulting in 510 offices that were closed for several hours or a full day.[30] Consequently, contract guard shortages negatively affected the agency's ability to serve the public, specifically vulnerable populations that needed assistance.

FPS officials said that open posts are due to security guard contractors hiring insufficient personnel to meet contract guard requirements to meet regional needs. However, security guard contractors said they face

[29]Federal Protective Service, *Federal Protective Service Post Tracking System, Protective Security Officer Vendor Guide*, Version 3.0. (Washington, D.C. May 4, 2022).

[30]SSA officials estimated in the last three years, there were approximately 15,000 hours that posts were unguarded by FPS contract guards.

challenges in recruiting, training, and retaining contract guards. According to FPS officials, they prioritize open posts and address this issue with security guard contractors through corrective action plans.

Training and Academy Management System (TAMS)

FPS implemented TAMS in 2019 to allow FPS personnel to track, monitor, and verify training records for FPS's contract guard workforce. Also, contract guard companies use TAMS to enter and update guard training and certification information, along with supporting documentation, such as electronic copies of training and certification records. FPS staff conduct oversight of guard training using TAMS. According to some FPS officials, TAMS is an improvement over the previous process, which did not provide a consolidated source for guard training records. However, other FPS officials have found the database inefficient in completing tasks because of data reliability and technology issues. While the system has been in use for more than 5 years, FPS officials said TAMS guidance and directives remain in draft form. FPS officials said the guidance and directives will be submitted to the policy review process by the end of fiscal year 2024.

- **TAMS data reliability.** Stakeholders identified data issues that affect the quality of data in TAMS, including missing data for contract guards and a lack of controls to verify that vendors provided guards with required training. According to FPS headquarters, regional, and union officials, because TAMS depends on contractors to upload training records, that information could be susceptible to human input errors or manipulation. FPS officials cannot use this database independently to verify the accuracy of the training data for contract guards. Union and FPS officials said they still need to collect additional data from security guard contractors to have a complete picture of compliance with training requirements. For example, FPS reported 13,377 active contract guards in TAMS as of April 2024, but TAMS' training records do not reflect the necessary levels of training or documentation for all contract guards on staff.

  FPS officials said there were various reasons for not having training records for all 13,377 active contract guards. One reason is that security guard contractors had not entered all the records into TAMS. Another reason is that all contract guards had not yet completed the training courses and not all courses are mandatory. Furthermore, following our covert testing, we requested training records for the contract guards at the facilities that did not detect our prohibited items. FPS officials said they could not provide training records for some contract guards who were on duty during the time of our covert testing. FPS officials could not identify the appropriate contract guards

on post based on PTS records, which identify the contract guards on duty. Officials said that since PTS has not been deployed to all guard contracts, they could not identify the names of the contract guards from PTS. Consequently, they could not collect the training and certification records for those contract guards in TAMS. FPS officials said if GAO had provided the names of the contract guards at the covert testing locations, they could have provided the training records for those contract guards. We did not gather the names of individual guards during our covert testing, since the purpose of the audit was to review FPS efforts to improve detection and data systems, not to investigate individual guard performance.

- **TAMS system design.** When conducting required quarterly training audits, FPS officials must access different parts of TAMS to confirm contract guard training requirements are met. This process is inefficient because it increases the time needed to complete each audit for thousands of contract guards. Some FPS staff said this design flaw makes it more time-consuming and difficult to use TAMS than traveling to the contractor's site to audit training files by hand, as they did before TAMS.
    - An agency official said that while TAMS can collect a lot of information, it is poorly organized, affecting the system's performance and speed. For example, agency officials must confirm that contract guards have completed X-ray screening training, which produces a three-page report. According to a regional official, after running so many reports, the system runs out of storage space, and TAMS administrators must develop another file folder to save new reports. As a result, agency officials said they had to search five or six file folders to verify training information. Regional officials said it may take days to find pertinent information with a sluggish computer program.
    - Several regional officials also mentioned that completing their work efficiently is difficult because the program is not user-friendly. An FPS official who was responsible for implementing TAMS in FPS said (1) the system was not intended for its current use of documenting all training requirements and (2) there are limits to how much the system can be modified for current FPS needs. While FPS officials have not addressed issues identified by stakeholders, FPS officials told us they are working to develop initiatives to capture technological best practices and enhance TAMS.

In conclusion, as the agency responsible for protecting thousands of federal facilities nationwide, FPS relies heavily on more than 13,000 contract guards. Failure to keep prohibited items out of federal facilities can compromise the safety of the people who work in and visit them. Moreover, threats to federal facilities persist even as FPS is experiencing a shortage of staff to provide oversight for the contract guard workforce. Therefore, it is essential that FPS improve the guards' success rate in detecting prohibited items and provide oversight of the contract guard workforce. Again, we plan to finalize our review of FPS's efforts to improve detection and data systems and issue a report later this year.

We shared a draft of this statement with FPS, the Department of Treasury, the GSA, and the Social Security Administration. FPS provided technical comments, which we incorporated as appropriate. The remaining agencies informed us that they had no comments.

Chairman Perry, Ranking Member Titus, 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 Acknowledgments

If you or your staff have any questions about this testimony, please contact David Marroni, Director, Physical Infrastructure, at (202) 512-2834 or MarroniD@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 statement are Keith Cunningham (Assistant Director); Nelsie Alcoser (Analyst in Charge); J. Howard Arp; Caroline Christopher; Brendan Culley; Peggie Garcia; Geoff Hamilton; Melissa Hart; Nicholas Lessard-Chaudoin; Jodi Lewis; Mark MacPherson; Robyn McCullough; Sarai Ortiz; Patricia Powell; Malika Rice; Kelly Rubin; Jeanne Sung; Kevin Walsh; Michelle Weathers; and Angel Zollicoffer.