United States Government Accountability Office

Report to Congressional Requesters

May 2023

FEDERAL FACILITIES

Improved Oversight Needed for Security Recommendations

Accessible Version

GAO-23-105649

GAO Highlights

Highlights of GAO-23-105649, a report to congressional requesters

May 2023

FEDERAL FACILITIES

Improved Oversight Needed for Security Recommendations

Why GAO Did This Study

FPS protects over 9,000 federal facilities with over 1.4 million employees and visitors. As part of its services, FPS conducts facility security assessments and recommends countermeasures to help address vulnerabilities at federal facilities. FPS conducts these assessments based on ISC security standards. Agencies are responsible for acting on these countermeasures.

GAO was asked to review the implementation of countermeasures recommended by FPS. This report (1) identifies information that FPS maintains on its assessments and recommendations, (2) identifies factors that affect agencies' decisions to act on these recommendations, and (3) examines how ISC assesses compliance with its security standards and countermeasures.

GAO reviewed FPS guidance on the information collected from its assessments, and how that information is entered into its database. In addition, GAO held discussion groups with officials representing 27 selected facilities where FPS conducted security assessments between 2017 and 2021, as well as FPS and ISC officials. GAO also reviewed ISC documentation and guidance.

What GAO Recommends

GAO is making two recommendations to DHS that it improve its oversight ability to (1) assess countermeasure implementation and (2) identify the acceptance of risk at facilities where recommended countermeasures are not implemented. DHS concurred with GAO's recommendations.

View GAO-23-105649. For more information, contact Catina Latham at (202) 512-2834 or lathamc@gao.gov.

What GAO Found

The Federal Protective Service (FPS) conducts security assessments and recommends countermeasures—such as security cameras—to address vulnerabilities at federal facilities. FPS maintains a database with information on its assessments and on agencies' decisions to approve or reject these recommendations. As GAO reported in 2022, FPS data indicate that agencies did not respond to over half of FPS's recommendations in fiscal years 2017 through 2021 (GAO-22-106177).

In the discussion groups GAO held with facilities' representatives, participants cited several reasons why agencies might not act on FPS recommendations. Reasons included the cost or feasibility of implementing recommended countermeasures.

Security Cameras as an Example of a Facility Countermeasure

Source: titikul_b/stock.adobe.com. | GAO-23-105649

The Interagency Security Committee (ISC), established by Executive Order 12977, is required to oversee the implementation of appropriate countermeasures in certain federal facilities, among other responsibilities. The Department of Homeland Security (DHS) chairs this organization, which is comprised of 66 federal agencies The ISC requires non-military executive branch agencies to self-report some information on the degree to which they comply with ISC's federal security standards. For example, these agencies report on the extent to which they documented their acceptance of risk for countermeasures they did not implement. However, GAO found that ISC's oversight does not verify that these agencies have:

- implemented FPS-recommended countermeasures, or
- documented the acceptance of risk for those countermeasures they do not implement at their facilities.

Without an oversight mechanism to verify if these federal facilities are implementing the appropriate countermeasures or accepting the risk of not doing so, the federal government lacks reasonable assurance that such facilities are secure.

Contents

Abbreviations

DHS Department of Homeland Security
FPS Federal Protective Service
FSL Facility security level
ISC Interagency Security Committee

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 8, 2023

The Honorable Glenn Ivey
Ranking Member
Subcommittee on Oversight, Investigations, and Accountability
Committee on Homeland Security
House of Representatives
The Honorable J. Luis Correa
House of Representatives

The Federal Protective Service (FPS), located within the Department of Homeland Security (DHS), protects over 9,000 federal facilities with more than 1.4 million employees and visitors. As part of its services, FPS conducts facility security assessments and recommends countermeasures, such as security cameras, to help prevent security incidents and address vulnerabilities at federal facilities. FPS conducts these assessments based on the federal security standards established by the Interagency Security Committee (ISC), a DHS-chaired organization of 66 federal departments and agencies. The ISC is responsible for developing security standards and overseeing the implementation of countermeasures, among other things, to enhance the quality and effectiveness of the security of federal facilities.[1] In addition, the federal agencies that occupy FPS-protected facilities play a key role in protecting these facilities.[2] Specifically, these agencies are responsible under ISC standards for acting on the countermeasures recommended by FPS to address security vulnerabilities.

FPS data indicate that agencies act on a small percentage of these recommendations, raising questions about the extent to which those federal facilities and their occupants are protected. Furthermore, at a

[1]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, 60 Fed. Reg. 54411 (Oct. 19, 1995), as amended by Executive Order 13286, 68 Fed. Reg. 10619 (March 5, 2003). This report refers to executive branch buildings and facilities in the United States occupied by federal employees for nonmilitary activities as “federal facilities.”

[2]Non-military executive branch agencies and departments are required under Executive Order 12977 to cooperate and comply with ISC policies and recommendations. Executive branch agencies and departments are exempt from complying with ISC policies and recommendations if the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods.

hearing in September 2022, congressional members raised concerns that there was limited oversight of the implementation of the recommended countermeasures.[3] Federal facilities have been the subject of numerous GAO reports and are included on GAO's list of high-risk areas in part due to security issues.[4]

You asked us to review issues related to the implementation of security countermeasures recommended by FPS at the federal facilities it protects. This report

- identifies the information FPS maintains on its assessments and its recommended countermeasures;
- identifies the factors that affect agencies' decisions to act on FPS recommendations; and
- examines how the ISC assesses compliance with its security standards and countermeasures at federal facilities.

To identify the information FPS maintains on its assessments and recommended countermeasures, we reviewed FPS guidance on the process for conducting facility security assessments. Specifically, we reviewed the FPS manual governing the information collected and entered into its risk assessment tool, a database also known as the Modified Infrastructure Survey Tool. In addition, we reviewed FPS's processes for how it records the information. We also interviewed FPS officials and inspectors who conduct the assessments and use the database.

To identify the factors that affect agencies' decisions to act on FPS recommendations, we obtained and analyzed the views of tenant agency officials who make decisions on those recommendations. To do this, we held six GAO-led discussion groups with representatives from 27 selected facilities, representing 14 agencies, where FPS made countermeasure recommendations between fiscal years 2017 and 2021. Each selected facility was represented by one participant. We selected a mix of facilities to ensure variation in a number of factors, such as the number of federal agencies located at the facility; the number of FPS recommended countermeasures for the facility; the percentage of recommendations with decisions (approved or rejected); and the number of recommendations

[3]*Federal Building Security: Examining the Risk Assessment Process, before the Subcommittee on Oversight, Management, and Accountability*, 117th Cong. (2022).

[4]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).

without a decision.[5] We received a list of contacts of the facility security committee chair or designated official at each facility, and used that to identify participants for the discussion groups.[6]

During our discussions we obtained information on the processes the participants used and the factors they consider when making decisions about FPS recommended countermeasures. We analyzed the responses to identify the most frequently cited factors among the discussion groups. Results from our analysis are not representative of all facilities but are intended to provide insights into issues affecting different facilities. We also held interviews with FPS inspectors from some of these locations to discuss their perspectives on interactions with agency representatives and reasons why responses were not provided for recommendations.

To examine how the ISC assesses compliance with its security standards and countermeasures at federal facilities, we reviewed ISC documentation and guidance on its compliance and verification processes, including the results of its most recent compliance reporting in 2021. In addition, we interviewed ISC officials about their efforts to provide oversight on agency compliance with the ISC standards and their process for verifying members' compliance reporting. We compared the ISC's oversight efforts to the oversight responsibilities outlined in Executive Order 12977, which established the ISC.

We conducted this performance audit from January 2022 to May 2023 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.

[5]We did not include facilities rated at the highest facility security level given the relatively small number of recommendations FPS made for these facilities during our evaluation period.

[6]Facility security committee chairs are the heads of a facility security committee, which votes on whether to implement FPS's recommended countermeasures from the facility security assessment for a facility with multiple tenant agencies. Designated officials are the representatives with the authority to address security recommendations for a single-tenant facility's security. For the purposes of this report, we refer to these officials or their designees as "tenant agency representatives."

Background

Federal Roles and Responsibilities

FPS is the agency primarily responsible for protecting federal employees and visitors in federally owned or leased facilities that are under the custody and control of the General Services Administration.[7] As part of FPS's responsibilities, FPS conducts facility security assessments of about 9,000 civilian federal facilities. These assessments identify security vulnerabilities and recommend countermeasures—such as security cameras, physical access control systems, and x-ray screening equipment—aimed at preventing security incidents. FPS, as an executive branch agency, is required to follow federal security standards when conducting facility security assessments.

The ISC is a DHS-chaired organization responsible for developing federal security standards to enhance the quality and effectiveness of security in and protection of civilian federal facilities.[8] The ISC was established within the executive branch and is comprised of 66 federal departments and agencies. Executive Order 12977 requires executive branch departments and agencies to cooperate and comply with the ISC's policies and standards. The Executive Order establishing the ISC directs it to:

1. establish policies for security in and protection of federal facilities;
2. develop and evaluate security standards for federal facilities;
3. develop a strategy for ensuring compliance with such standards; and
4. oversee the implementation of appropriate security measures—also referred to as countermeasures—in federal facilities.

As part of its responsibilities, the ISC developed security standards that define the criteria and processes agencies are to use in determining the

[7]DHS' statutory authority charges the Secretary with the protection of all federal facilities and property. FPS provides protection for General Services Administration facilities, as well as other non-General Services Administration facilities that pay fees to FPS for its protection. Most federal departments and agencies are generally responsible for protecting their own facilities and have physical security programs in place to do so. The number of federal civilian facilities protected by FPS is a small portion of the over 100,000 executive branch, non-military, federal buildings.

[8]The Interagency Security Committee is chaired by an official within the Cybersecurity and Infrastructure Security Agency via a delegation from the Secretary of DHS, and is housed within the Cybersecurity and Infrastructure Security Agency.

appropriate security level for a facility. These standards also established the appropriate countermeasures for federal facilities based on their security level (see fig. 1).

Figure 1: The Interagency Security Committee's Risk Management Process

Source: GAO analysis of Interagency Security Committee information. Image Montri/stock.adobe.com. | GAO-23-105649

Text of Figure 1: The Interagency Security Committee's Risk Management Process

- **Determine Facility Security Level (FSL)**
  - Tenant agencies make FSL determinations—which range from level I to level V, lowest to highest—based on five weighted security evaluation factors and the option for an intangible adjustment if warranted.
- **Identify the facility's baseline countermeasure**
  - Tenant agencies identify the set of baseline countermeasures associated with the facility's FSL. These countermeasures range from "minimum" for level I facilities to "very high" for level V facilities and must be met until a risk assessment is performed by the Federal Protective Service (FPS).
- **Identify and assess risk**
  - FPS conducts a facility security assessment to identify and assess risks. The risk assessment methodology must be credible, reproducible, and defensible; addressing three factors (threat, vulnerability, and consequence) for each undesirable event.
- **Determine necessary countermeasures**
  - FPS assesses the set of protective countermeasures to mitigate the risk of an undesirable event. If the risk is higher or lower than the level of protection afforded by the baseline countermeasures, FPS recommends changes to the countermeasures to meet the level of assessed risk.
- **Implement protective measures and/or accept risk**
  - Tenant agencies determine whether the recommended countermeasures are achievable. If so, set a timetable for countermeasure implementation. If not—e.g., due to physical limitations—consider alternate locations and/or accept unmitigated risk. Agencies must document decisions. In particular, decisions to accept risk should include alternative strategies considered or implemented, and opportunities in the future to implement needed countermeasures.
- **Measure performance**
  - Federal departments and agencies set performance measures that are based on agency mission, goals, and objectives to assess and document the effectiveness of the security program against these measures.

Source: GAO analysis of Interagency Security Committee information. Image Montri/stock.adobe.com. | GAO-23-105649

The ISC standards also establish the security-related responsibilities for tenant agencies. Specifically, the standards require that a facility security committee with representatives from each tenant agency be established in facilities with multiple tenant agencies. These facility security committees are responsible for addressing the facility-specific security issues identified in a security assessment and act on recommendations by approving or rejecting a recommended countermeasure. The tenant agencies are responsible for funding and implementing approved countermeasures. The tenant agencies provide the funds for the approved measures based on their share of the federally leased space they occupy in the facility. According to the ISC standards, each agency is required to pay its share of an approved countermeasure.[9] ISC standards state that tenant agencies that do not take action on a recommended countermeasure accept the risk of not implementing the countermeasure and require agencies to document the decision and rationale for accepting the risk.[10]

FPS's Facility Security Assessment Process

One of FPS's key security responsibilities is to conduct facility security assessments of federal facilities every 3 to 5 years to identify and assess potential risks. FPS inspectors evaluate a facility's existing countermeasures against the ISC's standards for the applicable facility security level. These measures are based on the necessary level of protection to mitigate the identified risk.[11] The inspector then recommends countermeasures and practices necessary to meet the appropriate security standards for the facility.

After completing the facility security assessment, the FPS inspector presents the report, including its recommended countermeasures, to the facility security committee. The ISC standards call for the committees to consider FPS's recommendations and decide whether to approve or

[9]For example, if an agency leases 75 percent of a facility, it is required to pay 75 percent of the total cost of the countermeasure. The agency or agencies leasing the other 25 percent of the facility would pay the remainder of that cost.

[10]The ISC defines risk acceptance as the explicit or implicit decision not to take an action that would affect all or part of a particular risk. ISC standards state that risk acceptance shall be provided to the headquarters security office.

[11]The ISC defines facility security levels on a scale from level I (lowest risk) to level V (highest risk).The facility security level is determined by the facility security committees after an assessment of security criteria.

disapprove (reject) the recommendations within 45 days.[12] The standard also states that the committees may accept the risk of not implementing a recommended countermeasure and must document the acceptance of that risk.

Once the facility security committee makes the decision to approve or reject each recommended countermeasure, the committee provides that decision to FPS. If no decision is provided to FPS within 45 days, FPS guidance directs the inspector to record a status of "no response" for the recommendation into its risk assessment database.

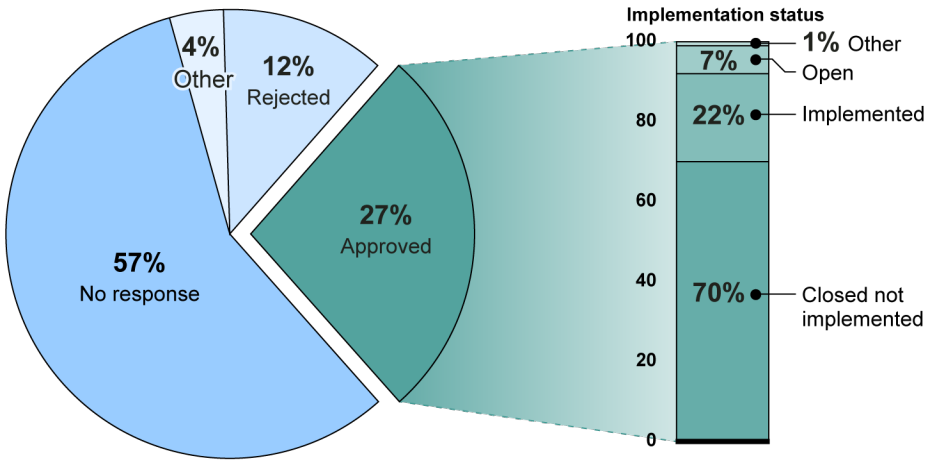
Status of FPS Recommended Countermeasures

In September 2022, we reported that in fiscal years 2017 through 2021, FPS made more than 25,000 security recommendations at nearly 5,000 federal facilities.[13] We found that the data indicate that FPS received a decision from the facility security committees on 43 percent of the recommendations made during that time period. We reported that the data indicated that FPS did not receive notification of the committees' decisions to approve or reject 57 percent of the 25,000 security recommendations. In addition, we found that while FPS data showed committees approved 27 percent of the FPS recommended countermeasures, FPS data indicate that most of those countermeasures were not implemented (see fig. 2).

[12]If committee members need additional time to review the assessment and recommended countermeasures, the committee chair may grant 45 days for review, in accordance with the ISC standards.

[13]GAO, *Federal Protective Service: Many Approved Security Recommendations Were Not Implemented and Preliminary Work Suggests Law Enforcement Deployments Have Increased*, GAO-22-106177 (Washington, D.C.: Sept. 22, 2022).

Figure 2: 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-23-105649

Data table for Figure 2: Facility Security Committees' Responses and Implementation Status of Approved Security Recommendations, Fiscal Years 2017–2021

	No response (in percent)	Other (in percent)	Rejected (in percent)	Approved (in percent)
FPS's Modified Survey Tool	57	4	12	27

	Other (in percent)	Open (in percent)	Implemented (in percent)	Closed not implemented (in percent)
Of the 27 percent approved implementation status for FPS's Modified Survey Tool	1	7	22	70

Source: GAO analysis of data from FPS's Modified Infrastructure Survey Tool. | GAO-23-105649

Note: "Other" includes recommendations that the Federal Protective Service (FPS) replaced with alternatives and recommendations that did not require a Facility Security Committee response.

As we previously reported, as of September 2022, FPS data showed that of the 27 percent of the recommendations approved by the committees, about 22 percent (about 1,500), were implemented. FPS recorded 70 percent of the approved recommendations as closed, but not implemented.

FPS Maintains Security Information for Facilities, Including Information on Decisions about Countermeasures

Our review of FPS's database found that FPS maintains information from its facility security assessments, as well as information on how agencies responded to FPS' recommended countermeasures. For example, inspectors record details such as the facilities' location, existing countermeasures, and local crime statistics. Additionally, inspectors record information about the existence of security documents for the facility including written security plans, occupant emergency plans, and active threat plans. The database also contains the previous assessment, including the vulnerabilities and threats that were identified and the recommended countermeasures. To complete the assessments, standardized questions in the database lead the inspectors through each area of facility security to identify security vulnerabilities. These areas range from entry control to lighting to fences. FPS inspectors develop recommended countermeasures appropriate to the necessary level of protection to mitigate the identified risk.[14]

FPS inspectors also collect and record facility security committee decisions for each recommendation in the database. Specifically, the database maintains information on committee decisions to approve or reject FPS recommendations, as well as the implementation status of recommended countermeasures approved by the committees. For the recommendations where the facility security committee did not provide a decision to FPS, the inspector records a status of "no response" into the database.

According to FPS officials, tenant agencies have access to the information in the database for their facilities and can view the status of security recommendations and countermeasures. FPS officials told us that agencies can also obtain access to FPS's information for all of their facilities, enabling them to take a broader portfolio approach to security decisions. The database provides FPS a standardized way of collecting and reporting facility information to allow for informed decisions regarding countermeasures and inventory management.

[14]Information on the types of vulnerabilities identified by FPS in fiscal year 2017 through 2021 can be found in our report, GAO-22-106177.

Discussion Groups Identified Several Factors, Including Cost, That Affected Decisions to Act on Recommendations

Cost, Expertise, and Feasibility Were Most Frequently Identified as Factors for Not Acting on Recommendations

In our six discussion groups, tenant agency representatives identified several factors, including cost, that contributed to their decisions for not acting on FPS recommendations. The facility security committees act on a recommendation by approving or rejecting a recommended countermeasure and implementing or not implementing a countermeasure.

In all six of the discussion groups we held, participants mentioned that the expenses associated with purchasing and installing countermeasures recommended by FPS affected committee decisions. Recommended countermeasures can range from no cost to the tenants to over $1 million. For example, a recommendation to improve blast protection on the windows of one facility had an estimated cost of $1.8 million. In two discussion groups, participants stated the committees would often approve and implement recommendations with little to no expense, such as replacing lighting to improve illumination at an entrance or trimming trees that obscure security cameras. According to participants in these groups, the more expensive countermeasures were often not approved.

Furthermore, the availability of funding or budgetary considerations were mentioned as a factor affecting committee decisions on FPS recommendations in all six discussion groups. For example, in four discussion groups, participants stated that in facilities with multiple tenant agencies, coordinating funding can affect decisions to approve and implement countermeasures. In four of the discussion groups, participants stated that not all of the tenant agencies in their facilities could obtain or secure funding for the recommended countermeasure. According to these participants, without all tenant agencies paying their share of an approved countermeasure, the countermeasure will not be implemented.

There are some instances where a facility security committee may fund part of a countermeasure recommended by FPS. Specifically, in three groups, participants noted that the committee might not approve a recommended countermeasure because of costs but might implement

part of the recommendation. In one discussion group, participants noted that their committees balance available funding with the risk of not implementing a recommended countermeasure. For example, one participant stated that the facility security committee approved fewer cameras at the facility than the number recommended by FPS in its security assessment because the agencies did not have funding available to install all the cameras. Instead, the committee approved several cameras that would cover facility entrances, to address the areas they considered the highest security risk. According to the participant, while taking action to partially implement a recommendation may not meet the necessary countermeasures, it can improve facility security.

In addition to cost, participants from the discussion groups identified other factors that influence facility security committee decisions to approve or reject FPS recommendations. Additional factors frequently cited by discussion groups were:

- **Knowledge and expertise.** In five of the discussion groups, participants stated that knowledge and expertise of federal security standards can help facility security committees make decisions on FPS recommendations.[15] In four discussion groups, participants noted that they found assistance and expertise from their agencies' security specialists helpful in making these decisions on the FPS recommendations. In four groups, participants noted that these security specialists within their agencies provide advice regarding security requirements and countermeasures. In these groups, participants stated that these experienced officials help the facility security committee representatives understand the recommendations and make informed decisions.

  In all of the discussion groups, participants noted (when we asked) that training on the facility security committee responsibilities and the ISC standards would be helpful for committee representatives to perform their duties. However, in five discussion groups, at least one participant said they did not receive training about their responsibilities as a facility security committee chair. The ISC standards require training for facility security committee members on the committee responsibilities and the ISC's security standards. The ISC provides in-person and virtual training, as well as independent study courses for facility security committee members to meet its training requirements.

[15]The ISC recommends that facility security committee representatives should consult their respective headquarters' security element if the representative needs technical advice.

As discussed later in this report, the ISC is evaluating agency compliance with its training requirements.

- **Feasibility and usefulness.** In five of the discussion groups, participants mentioned that their facility security committees considered how feasible and useful it would be to implement the recommended countermeasure at their respective facility. Specifically, physical limitations of the facility—such as space limitations or the age of a facility—have prevented the facility from installing a certain recommended countermeasure, according to participants in three discussion groups. According to FPS guidance, the security assessments compare the countermeasures in place at a facility against the ISC security standards to recommend appropriate countermeasures.[16] These standards apply even if the facility space cannot accommodate the countermeasure. The ISC standards state it is the responsibility of the tenant agencies to determine if the implementation of countermeasures is feasible and cost-effective. If the tenant agencies decide to reject the recommended countermeasure, they must identify the highest level of achievable countermeasure to mitigate the risk or document the acceptance of risk.

A Variety of Reasons Were Identified for Not Responding to FPS Recommendations

In the discussion groups we held, participants noted several reasons for why a facility security committee might not respond to an FPS recommendation. As we reported in September 2022, FPS data suggest that tenant agencies do not provide a decision to FPS on more than 50 percent of its recommendations.[17] In four discussion groups, participants noted that the 45-day requirement to respond is not a reasonable timeframe to make a decision, with some citing the need for additional time for expensive and more complex countermeasures. For example, in one discussion group, a participant noted it takes more than 45 days to schedule a meeting with multiple tenant agency representatives, to solicit and review estimates to install the countermeasure, and to discuss the proposed estimates as a committee in order to make an informed decision.

[16]The facility countermeasures should be compared to the necessary level of protection identified as part of the ISC risk management process.

[17]GAO-22-106177.

Additionally, in two discussion groups, participants stated that communication issues between the facility security committee and FPS inspectors may result in the committee not responding to FPS. Specifically, these participants stated that turnover in officials serving as the committee chair or among FPS inspectors resulted in missing or delayed correspondence with FPS. In one instance, a participant noted that after the chairperson left the agency, correspondence with FPS was not shared with the new chair and delayed some decisions.

FPS inspectors we interviewed cited additional reasons that may delay responses or lead to no response from facility security committees. According to these inspectors, because serving on the committee is a collateral duty, members have competing priorities and may not prioritize responding to FPS about the recommendations. Further, according to the inspectors, when they present the results of their assessment to the facility security committee, if the recommendations are not approved and implemented, the agencies are accepting the security risk. They said that committees may not respond because they are reluctant to attribute their names to a rejected recommendation and the associated risk. The committees may not understand that it is their agency and not them personally taking on the risk since as committee members they are acting as representatives of their agency, according to the inspectors we interviewed.

ISC Assesses Compliance with Its Standards but Does Not Verify Countermeasure Implementation

The ISC Assesses Compliance with Its Facility Security Standards

The ISC uses an annual questionnaire to assess federal compliance with its policies and standards for developing a process to identify, assess, and prioritize security risks at federal facilities.[18] Starting in calendar year 2019, the ISC requires federal departments and agencies to self-report the degree to which they have implemented ISC policies and standards.

[18]The annual self-reported questionnaire includes questions for compliance with ISC policies and standards at the department and agency level, as well as compliance at individual federal facilities.

The departments and agencies respond to a series of questions ranging from organizational compliance with guidance and policies to specific facility compliance with ISC standards.[19] For example, organizational-compliance questions ask about the extent to which the departments and agencies established policies that comply with the ISC's standards. Facility-compliance questions ask about the actual application of the ISC's standards at the specific facility, such as whether the facility established a facility security committee and whether the committees maintain documentation for their meetings.

ISC officials said that the self-reported data indicate that departments and agencies have generally established guidance and policies that align with ISC standards, but the standards are less often met at the facility level. According to the ISC, in 2021, all but one department or agency self-reported its level of compliance with ISC organizational standards.[20] These departments and agencies also reported on about 70 percent (about 11,000) of their individual facilities. According to the ISC, in 2021 the average self-reported organizational compliance score has improved since 2019, but the facility scores have not improved during the same time period.[21] The ISC added that the lack of improvement in facility scores is likely a result of more facilities reporting since 2019.

ISC officials said they are using the results of the compliance reporting to identify the need for additional or clarified policies and guidance. For example, based on low compliance scores, the ISC developed guidance documents that agencies can use to establish processes related to prohibited items at their facilities.[22] ISC officials also explained that they have developed reports that allow agencies to see how their organizational compliance responses compare to the results of all organizations' scores on specific benchmarks. Our review of the self-

[19]Organizational-compliance questions are filled out at the headquarters and sub-organization level. According to ISC officials, a sub-organization is a smaller component of a federal department (for example, this can include either a department agency or an agency regional office). This designation is determined by how each department organizes its components. For the purpose of this report, we refer to all organization and sub-organization components as departments and agencies.

[20]ISC reported that it received responses from 215 federal organizations and sub-organizations to its organizational compliance questions for calendar year 2021.

[21]The organizational and facility compliance is measured on a 5-point scale, based on an average calculated from the responses to the ISC questionnaire.

[22]ISC standards provide that facilities should develop policies and procedures detailing the control of prohibited items, which includes firearms, weapons, explosives, or other destructive devices, into federal facilities.

reported data showed that several of the issues identified in our discussion groups were reflected in low compliance in related requirements. For example, in line with many discussion groups' concerns about the difficulty of reaching agreement within the facility security committee about acting on recommendations, most departments and agencies reported they were in the process of developing written procedures to assist the facility security committees in resolving issues. Furthermore, in five of the discussion groups, participants noted a lack of training for facility security committee chairs, and most departments and agencies also reported less than two-thirds of committee members had completed required training.

Beginning in fiscal year 2023, the ISC plans to verify departments' and agencies' self-reported organizational compliance with ISC policies and standards. The ISC developed a risk-based approach to select 14 departments and agencies to undergo this verification each year. The ISC considered a number of risk factors when making its selection, including threats based on the departments' and agencies' mission and vulnerabilities and on self-reported compliance with ISC standards. The ISC plans to verify the self-reported organizational compliance responses by reviewing the selected departments' and agencies' policies, procedures, and supporting documentation. As of February 2023, ISC officials told us that they are developing a pilot to verify facilities' self-reported compliance with ISC standards and policies, and that they plan to test this process on five facilities in the fourth quarter of fiscal year 2023.

The ISC Does Not Verify the Implementation of FPS Recommended Countermeasures at Federal Facilities

Our review of the ISC's oversight mechanisms found that the ISC does not verify the implementation of appropriate countermeasures at federal facilities through its annual organizational or facility compliance reporting. In addition, ISC's verification process does not verify the acceptance of risk for countermeasures that are not implemented in federal facilities. Executive Order 12977 directs the ISC to oversee the implementation of appropriate countermeasures in federal facilities, among other responsibilities.

As previously discussed, the ISC relies on an annual questionnaire to conduct oversight. However, the questionnaire does not include questions on the extent to which departments and agencies implement FPS recommended countermeasures at facilities or the number of

countermeasures implemented at a facility. In addition, the self-reported questionnaire does not solicit information on how many recommended countermeasures that facilities do not implement. It also does not verify that federal facilities document the acceptance of the risk of not implementing countermeasures at the facility level. Instead, the questionnaire asks how often (never, sometimes, often, usually, or always) departments and agencies, as well as their facilities, document the accepted risk of not implementing recommended countermeasures, among other decisions.[23] However, our review of the self-reported data from ISC's questionnaire indicate that not all departments or agencies and their facilities document the decisions to accept the risk of not implementing countermeasures, as required by ISC standards.

As the interagency committee tasked with developing a strategy to assess compliance with security standards and overseeing the implementation of countermeasures, the ISC is uniquely positioned to oversee this information from federal facilities. As noted above, ISC officials told us they plan to conduct a pilot to verify select facilities' compliance at the end of fiscal year 2023. However, the pilot will be limited to five facilities and will not assess the countermeasures implemented at a facility or identify the countermeasures for which the facility accepted the risk of not implementing them. ISC officials stated that they do not plan to verify the implementation of countermeasures at federal facilities because departments and agencies are responsible for tracking their own facilities and monitoring the results of their risk assessments. ISC officials also noted that they could not verify the responses of all federal facilities, given ISC staff size and other responsibilities. However, ISC already obtains information from departments and agencies on their facilities through its questionnaire, and ISC officials told us they could potentially revise its annual questionnaire to obtain information on recommendation implementation and the instances in which facilities accept the risk of not implementing recommendations.

Without an oversight mechanism to verify if departments and agencies are implementing the appropriate countermeasures recommended by FPS or accepting the risk of not doing so, the federal government does not have reasonable assurance that its facilities are secure. As previously noted, FPS data indicate that tenant agencies do not provide a decision

[23]The questionnaire assigns a percentage for the responses of how often a facility documents the acceptance of risk for of unimplemented countermeasures. For example, a response of "sometimes" equates to approximately 25 percent of the time and "usually" equates to 75 percent.

to FPS on more than 50 percent of its recommendations. Therefore the implementation status of these recommended countermeasures is unknown. Further, facilities that do not meet the ISC's standards and implement recommended countermeasures may leave federal agencies exposed to risks in protecting their workforce, visitors, and federal facilities. Improving the ISC's oversight of implemented countermeasures and risk acceptance at federal facilities could provide a greater level of assurance that facilities are meeting the ISC's security standards, as well as better identify security risks to federal facilities.

Conclusion

Ensuring the appropriate countermeasures and practices are in place is the first line of defense for federal facilities to ensure the safety of employees and visitors. Tenant agencies rely on FPS to assess vulnerabilities to federal facilities and to recommend the appropriate countermeasures. However, data indicate that tenant agencies are neither making decisions on—nor are they implementing—many of the recommended countermeasures. The ISC has taken steps to verify compliance with its standards. However, its oversight does not verify the extent to which departments and agencies implement these countermeasures or document their acceptance of the associated risks for those they do not implement. Improved oversight mechanisms should enhance the federal government's ability to protect the more than 1.4 million federal employees and members of the public who visit federal facilities each year.

Recommendations for Executive Action

We are making the following two recommendations to DHS:

- The Secretary of Homeland Security should ensure that the Cybersecurity and Infrastructure Security Agency improves its oversight of security measures by modifying its compliance and verification process to assess the implementation of FPS's recommended countermeasures. (Recommendation 1)
- The Secretary of Homeland Security should ensure that the Cybersecurity and Infrastructure Security Agency improves its oversight of security measures by modifying its compliance and verification process to identify the recommendations for which

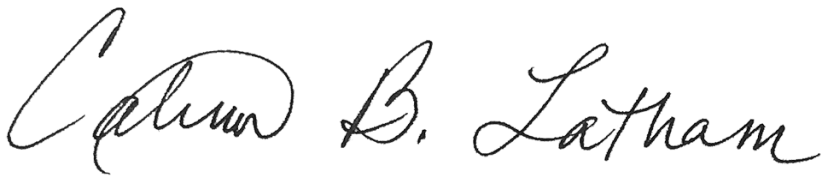
agencies did not implement the recommended countermeasure and did not document the acceptance of the risk. (Recommendation 2)

Agency Comments

We provided a draft of this report to DHS for review and comment. In its comments, reproduced in appendix I, DHS concurred with our recommendations. DHS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff any have questions about this report, please contact me 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 report. GAO staff who made key contributions to this report are listed in appendix II.



Catina B. Latham
Director, Physical Infrastructure

Appendix I: Comments from the Department of Homeland Security

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

Homeland Security

April 21, 2023

Catina B. Latham
Acting Director, Physical Infrastructure
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105649, "FEDERAL FACILITIES: Improved Oversight Needed for Security Recommendations"

Dear Ms. Latham:

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

DHS leadership is pleased to note GAO's positive recognition of the Federal Protective Service's (FPS) rigorous process for collecting, tracking and storing facility security assessments, which are used to make informed decisions on countermeasures. GAO also recognized the Cybersecurity and Infrastructure Security Agency's (CISA) planned efforts to verify compliance with Interagency Security Committee (ISC) standards. DHS remains committed to using its security expertise and the law enforcement authority, when appropriate, to protect federal government facilities and safeguard the millions of employees and visitors who pass through them every day.

Agencies are responsible for acting on security recommendations and funding and implementing approved countermeasures. This was reinforced in the recent update by the General Services Administration (GSA) of Title 41 of the Code of Federal Regulations Part 102-81.25 which states – "Each agency occupying a Federal facilities or Federal grounds under the jurisdiction, custody or control of GSA … is responsible for implementing, maintaining, and upgrading the physical security standards."[1] CISA began implementing the ISC's compliance program in 2019 and looks forward to maturing the program to assist agencies in fulfilling their security responsibilities.

[1] Subpart B – Physical Security does note some exceptions. See https://www.ecfr.gov/current/title-41/subtitle-C/chapter-102/subchapter-C/part-102-81

The draft report contained two recommendations for CISA with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.04.21 09:56:30 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

2

Enclosure: Management Response to Recommendations Contained in GAO-23-105649

GAO recommended that the Secretary of Homeland Security ensure that CISA:

Recommendation 1: Improves its oversight of security measures by modifying its compliance and verification process to assess the implementation of FPS's recommended countermeasures.

Response: Concur. CISA's ISC compliance program assesses adherence to standards through organizational and facility reporting, as well as independent verification. The ISC will review its current processes and update them to improve insight into the implementation of countermeasures. Specifically, CISA Infrastructure Security Division (ISD) will work with ISC members – which includes senior level executives from 67 federal departments and agencies – to update the annual questionnaire to include questions related to the implementation of recommended countermeasures, to include those from FPS. CISA will ensure that the questions added do not duplicate information already available in FPS's Modified Infrastructure Survey Tool. Estimated Completion Date (ECD): April 30, 2024.

Recommendation 2: Improves its oversight of security measures by modifying its compliance and verification process to identify the recommendations for which agencies did not implement the recommended countermeasure and did not document the acceptance of the risk**.**

Response: Concur. The ISC's annual questionnaire already includes questions related to the documentation for risk acceptance for any countermeasures not implemented. However, CISA ISD will be moving forward with a pilot for compliance verification at the facility-level to allow for independent verification of the self-reported survey compliance statistics. CISA will include verification of documentation as an element of its pilot for compliance verification. ECD: April 30, 2024.

3

Text of Appendix I: Comments from the Department of Homeland Security

April 21, 2023

Catina B. Latham

Acting Director, Physical Infrastructure

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105649, “FEDERAL FACILITIES: Improved Oversight Needed for Security Recommendations”

Dear Ms. Latham:

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

DHS leadership is pleased to note GAO’s positive recognition of the Federal Protective Service’s (FPS) rigorous process for collecting, tracking and storing facility security assessments, which are used to make informed decisions on countermeasures. GAO also recognized the Cybersecurity and Infrastructure Security Agency’s (CISA) planned efforts to verify compliance with Interagency Security Committee (ISC) standards. DHS remains committed to using its security expertise and the law enforcement authority, when appropriate, to protect federal government facilities and safeguard the millions of employees and visitors who pass through them every day.

Agencies are responsible for acting on security recommendations and funding and implementing approved countermeasures. This was reinforced in the recent update by the General Services Administration (GSA) of Title 41 of the Code of Federal Regulations Part 102-81.25 which states – “Each agency occupying a Federal facilities or Federal grounds under the jurisdiction, custody or control of GSA … is responsible for implementing, maintaining, and upgrading the physical security

standards."[1] CISA began implementing the ISC's compliance program in 2019 and looks forward to maturing the program to assist agencies in fulfilling their security responsibilities.

The draft report contained two recommendations for CISA with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-23-105649 GAO recommended that the Secretary of Homeland Security ensure that CISA:

Recommendation 1: Improves its oversight of security measures by modifying its compliance and verification process to assess the implementation of FPS's recommended countermeasures.

Response: Concur. CISA's ISC compliance program assesses adherence to standards through organizational and facility reporting, as well as independent verification. The ISC will review its current processes and update them to improve insight into the implementation of countermeasures. Specifically, CISA Infrastructure Security Division (ISD) will work with ISC members – which includes senior level executives from 67 federal departments and agencies – to update the annual questionnaire to include questions related to the implementation of recommended countermeasures, to include those from FPS.

[1] 1 Subpart B – Physical Security does note some exceptions. See https://www.ecfr.gov/current/title-41/subtitle- C/chapter-102/subchapter-C/part-102-81

CISA will ensure that the questions added do not duplicate information already available in FPS's Modified Infrastructure Survey Tool. Estimated Completion Date (ECD): April 30, 2024.

Recommendation 2: Improves its oversight of security measures by modifying its compliance and verification process to identify the recommendations for which agencies did not implement the recommended countermeasure and did not document the acceptance of the risk.

Response: Concur. The ISC's annual questionnaire already includes questions related to the documentation for risk acceptance for any countermeasures not implemented.

However, CISA ISD will be moving forward with a pilot for compliance verification at the facility-level to allow for independent verification of the self-reported survey compliance statistics. CISA will include verification of documentation as an element of its pilot for compliance verification. ECD: April 30, 2024.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Catina B. Latham, (202) 512-2834 or LathamC@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following individuals made important contributions to this report: Crystal Huggins, Assistant Director; Maria Edelstein, Assistant Director; John F. Miller, Analyst-in-charge; Susan Bernstein; Mallory Bryan; Melanie Diemel; Geoffrey Hamilton; Alicia Loucks; Minette Richardson; Amelia Shachoy; Elizabeth Wood; and Fralinda Zazay.

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