United States Government Accountability Office

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, November 29, 2023

FEDERAL FACILITIES

Continued Oversight of Security Recommendations Needed

Statement of David Marroni, Acting Director, Physical Infrastructure Team

GAO-24-107137

November 2023

FEDERAL FACILITIES

Continued Oversight of Security Recommendations Needed

GAO Highlights

Highlights of GAO-24-107137, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Managing federal real property has been on GAO's High-Risk List for 20 years, due in part to threats to federal facilities. Several agencies play an important role in ensuring that federal facilities have countermeasures in place. The ISC—chaired by the Department of Homeland Security (DHS)—is responsible for overseeing federal agency compliance with its policies and standards and the implementation of FPS-recommended countermeasures. Agencies are responsible for deciding whether to implement these countermeasures.

This statement discusses: (1) how the ISC assesses federal agency compliance with its policies and standards, (2) the implementation status of FPS-recommended countermeasures, and (3) actions the ISC is taking to assess the implementation of FPS-recommended countermeasures.

This statement is based primarily on GAO's September 2022 and May 2023 reports. In addition, this statement provides an update on actions the ISC has taken in response to GAO's recommendations.

What GAO Recommends

GAO made two recommendations in its May 2023 report, that DHS: (1) assess countermeasure implementation and (2) identify the acceptance of risk at facilities where recommended countermeasures are not implemented. DHS concurred with the recommendations. As of October 2023, DHS has not yet fully addressed these recommendations.

View GAO-24-107137. For more information, contact David Marroni at (202) 512-2834 or MarroniD@gao.gov.

What GAO Found

The Interagency Security Committee (ISC) establishes security policies and standards for non-military federal facilities. To assess compliance with these security policies and standards, the ISC reviews federal agencies' responses to an annual questionnaire. According to ISC officials, in fiscal year 2023, the ISC started to verify these self-reported responses to the questionnaire.

The Federal Protective Service (FPS) conducts security assessments and recommends countermeasures—such as security cameras—to help agencies address vulnerabilities at federal facilities. GAO found that federal agencies did not implement most of the 32,000 countermeasures FPS recommended from fiscal years 2017 through 2023. Specifically, FPS data indicate that agencies did not respond to more than half of FPS's security recommendations and implemented fewer than 1,800 recommendations during this period.

Security Camera, an Example of a Facility Countermeasure

Source: titikul_b/stock.adobe.com. | GAO-24-107137

As of October 2023, the ISC has taken some actions to assess whether agencies implemented FPS-recommended countermeasures at federal facilities—or whether they accepted risks for countermeasures not implemented—but has not yet fully addressed GAO's May 2023 recommendations to do so. Specifically, the ISC plans to update its annual questionnaire in 2024 to include the degree to which agencies have implemented countermeasures, including those recommended by FPS. In addition, as part of a fiscal year 2024 pilot, the ISC plans to verify the documentation of risk acceptance for countermeasures not implemented for 10 facilities.

Until the ISC completes its planned efforts to improve its assessment of agencies' and facilities' implementation of FPS recommendations, the implementation status of more than half of FPS's recommended countermeasures will remain unknown and the federal government may not have reasonable assurance that its facilities are secure.

Chairman Peters, Ranking Member Paul, and Members of the Committee:

I am pleased to be here today to discuss our work on the measures federal agencies take to secure their facilities. Twenty years ago, we placed managing federal real property on GAO's High-Risk List, in part, due to threats to federal facilities.[1] Recent incidents demonstrate that the security of federal facilities remains a high-risk area. For example, beginning in May 2020, violent protests at federal facilities in Portland, Oregon resulted in several injuries and extensive property damage. In another incident, in August 2022, an individual attempted to breach a Federal Bureau of Investigation office in Cincinnati, Ohio. Given these and other incidents, it is critical that federal agencies implement appropriate countermeasures—such as fences, access control systems, or cameras—to address vulnerabilities to facilities. We and congressional members have raised concerns about limited oversight over the implementation of recommended countermeasures at federal facilities.[2]

Several federal agencies play an important role in ensuring that federal facilities have countermeasures in place. The Federal Protective Service (FPS), located within the Department of Homeland Security (DHS), protects over 9,000 federal facilities and more than 1.4 million employees and visitors. As part of its services, FPS conducts facility security assessments and recommends countermeasures to federal agencies that occupy FPS-protected facilities. These agencies are responsible for deciding whether to implement the countermeasures recommended by FPS. The Interagency Security Committee (ISC), a DHS-chaired organization consisting of 66 members, including federal departments and agencies, establishes security policies and standards for federal

[1]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 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).

[2]*Federal Building Security: Examining the Risk Assessment Process, Before the House Committee on Homeland Security, Subcommittee on Oversight, Management, and Accountability*, 117th Cong. (2022).

facilities.[3] The ISC also oversees federal agency compliance with these policies and standards, and federal agency implementation of recommended countermeasures in non-military federal facilities.[4]

My statement today focuses on (1) how the ISC assesses federal agency compliance with its policies and standards, (2) the implementation status of FPS-recommended countermeasures, and (3) actions the ISC is taking to assess the implementation of FPS-recommended countermeasures. The statement is based primarily on reports we issued in September 2022 and May 2023. In the May 2023 report, we recommended that DHS take actions to improve its oversight of agencies' actions on FPS-recommended countermeasures.[5] My statement will update the status of federal agency implementation of FPS-recommended countermeasures and ISC's actions to address our recommendations, as of October 2023.

For our May 2023 report examining ISC's assessment of federal agencies' compliance with its polices and standards and the actions ISC is taking to assess the implementation of countermeasures, we reviewed ISC documentation and guidance on their oversight processes. We also interviewed ISC officials about their oversight of agency compliance with the ISC policies and standards and their verification of agencies' implementation of countermeasures at facilities. Additionally, for this statement, we interviewed ISC officials in October 2023 on the actions they had taken to implement recommendations we made in our May 2023 report.

[3]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 statement refers to executive branch buildings and facilities in the United States occupied by federal employees for nonmilitary activities as "federal facilities."

[4]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.

[5]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). GAO, *Federal Facilities: Improved Oversight Needed for Security Recommendations*, GAO-23-105649 (Washington, D.C.: May 8, 2023).

For our September 2022 report on the implementation of FPS-recommended countermeasures, we obtained data from FPS on recommendations it made to federal agencies on countermeasures from fiscal years 2017 through 2021. We analyzed the data to identify the status of federal agency approval and implementation of the recommendations. For this statement, we obtained and analyzed updated data from FPS on the approval and implementation status of recommendations through fiscal year 2023. We assessed the updated data against GAO data reliability standards, including checking the data for accuracy and completeness. We determined the data were sufficiently reliable for the purposes of describing the implementation status of FPS-recommended countermeasures. Additionally, for our 2023 report we led six discussion groups with agency representatives from 27 selected facilities, representing 14 agencies, to obtain views on factors that influenced decisions on FPS recommendations.[6] More detailed information on our objectives, scope, and methodology for our prior work can be found in our issued reports.

We conducted the work on which this statement is based 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.

Background

FPS is the agency primarily responsible for protecting civilian federal facilities that are under the custody and control of the General Services Administration.[7] As part of its responsibilities, FPS conducts facility security assessments of federal facilities every 3 to 5 years to identify and

[6]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; percentages of approved and rejected decisions; and the number of recommendations without a decision.

[7]DHS' statutory authority charges the Secretary with the protection of all federal facilities and property. 40 U.S.C. § 1315(a). FPS provides protection for General Services Administration facilities, as well as other federal facilities that pay fees to FPS. 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.

evaluate potential risks and vulnerabilities.[8] These assessments recommend countermeasures, such as fences, physical access control systems, and security cameras, to help prevent or mitigate security incidents. FPS provides its assessments to federal agencies that obtain space in facilities through the General Services Administration (known as tenant agencies), and records the scheduling, completion, and results of facility security assessments into its database. FPS also records the decisions of tenant agencies on whether they will implement the recommended countermeasures at federal facilities. If the tenant agencies do not provide a decision within 45 days, FPS records a status of "no response" in its database.

The 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.[9] These ISC standards define the criteria and processes to be used to determine the minimum physical security requirements and associated countermeasures for federal facilities based on the security level of the facility.[10] Executive Order 12977 requires executive branch departments and agencies to cooperate and comply with the ISC's policies and standards. Executive Order 12977 also directs the ISC to oversee the implementation of appropriate countermeasures in federal facilities. ISC standards require federal agencies to document the acceptance of the risk of not implementing recommended countermeasures.

Tenant agencies are responsible for making facility-specific security decisions, either through a facility security committee or a designated official. In a facility with multiple tenant agencies, ISC standards require the establishment of a facility security committee consisting of

[8]Other FPS responsibilities include overseeing Protective Security Officers (i.e., contract guards) who provide services such as screening visitors and responding to law enforcement incidents. In 2019, FPS developed two systems to oversee its contract guard workforce—one that tracks training and one that manages the contract guard workforce. In April 2023, we reported that facility security remains a high-risk area, in part because FPS had not fully implemented the system that manages the contract guard workforce. Also, we reported that the two systems are not yet fully interoperable. See GAO-23-106203.

[9]The ISC is chaired by an official from the Cybersecurity and Infrastructure Security Agency via a delegation from the Secretary of Homeland Security.

[10]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.

representatives from each tenant agency.[11] These committees are responsible for addressing facility-specific security issues identified in FPS's facility security assessments. The committees also consider FPS-recommended countermeasures and decide whether to approve or reject the recommendations. Tenant agencies are also responsible for funding and implementing approved countermeasures or accepting the risk of unimplemented recommendations.

The ISC Assesses Compliance with Its Standards by Reviewing Federal Agencies' Responses to an Annual Questionnaire

In May 2023, we reported that the ISC began using an annual questionnaire in 2019 to assess federal agencies' compliance with its policies and standards.[12] The annual questionnaire asks federal departments and agencies to self-report whether they comply with ISC policies and standards, and whether individual federal facilities comply with the standards. ISC officials told us that departments' and agencies' self-reported responses indicate they have generally established guidance and policies that align with ISC standards, but the standards are less often met at facilities.

ISC officials said they use the results of the annual compliance reporting questionnaire to identify the need for additional or clarified policies and guidance. For example, based on low compliance results, the ISC developed guidance documents that agencies can use to establish processes related to prohibited items at their facilities.[13] ISC officials also explained that they have developed reports that allow agencies to see how their responses compare to the results of all departments and agencies on specific benchmarks.

As we reported in May 2023, the ISC started to verify departments' and agencies' self-reported compliance with ISC policies and standards.[14] The ISC developed a risk-based approach to select the federal departments and agencies that will undergo the verification each year. Specifically, the ISC considered a number of risk factors when selecting departments and agencies, including threats and results of the self-reported questionnaire.

[11]In multi-tenant facilities, representatives from each tenant agency vote on whether to implement FPS's recommended countermeasures. In single-tenant facilities, designated officials are the representatives with the authority to address security recommendations.

[12]GAO-23-105649.

[13]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, in federal facilities.

[14]GAO-23-105649.

The ISC planned to verify self-reported responses by reviewing the selected departments' and agencies' policies, procedures, and supporting documentation. As of October 2023, ISC officials stated that they are completing this verification of 10 departments and agencies. In addition, ISC officials told us that they started a pilot to verify self-reported compliance with ISC standards and policies at 10 facilities. ISC officials stated that it will complete this pilot in fiscal year 2024.

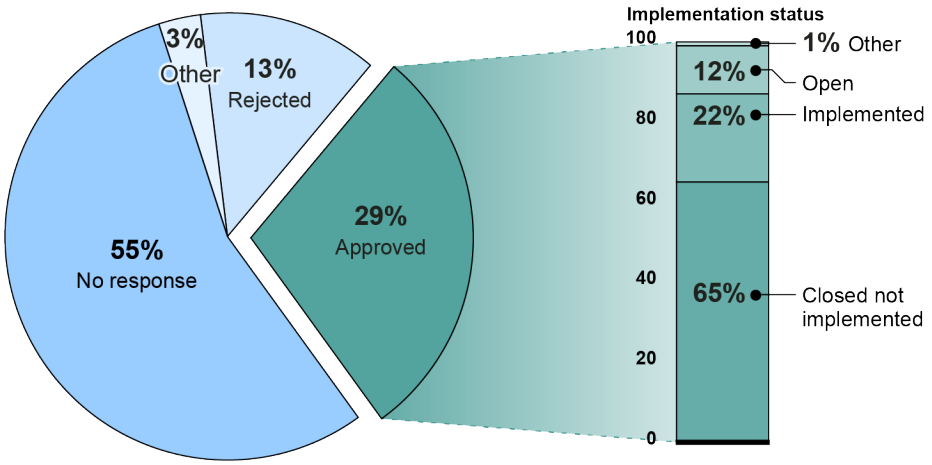
Federal Agencies Generally Have Not Implemented FPS-Recommended Countermeasures

Our analysis of FPS data found that federal agencies did not implement most FPS recommendations.[15] Between fiscal years 2017 and 2023, FPS made over 32,000 recommendations at over 5,000 federal facilities. These recommendations ranged from addressing physical vulnerabilities such as electronic security systems, barriers, and lighting, to ensuring facility practices meet appropriate standards.

FPS data indicate that facility security committees did not respond to more than half of FPS's security recommendations. We found that facility security committees approved 29 percent of the recommendations from fiscal year 2017 through 2023. We also found that, of the recommendations where FPS documented a date of approval in its system, agencies implemented 22 percent—or fewer than 1,800—recommendations at federal facilities as of October 2023 (see fig. 1).

[15]FPS recommends countermeasures for facilities. Facility security committees respond to FPS recommendations, and facility tenants are responsible for implementing them. These tenants can be federal departments or agencies. Throughout this section, we refer to these tenants as agencies.

Figure 1: Facility Security Committees' Responses to Federal Protective Service (FPS) Security Recommendations and Implementation Status of Approved FPS Security Recommendations, Fiscal Years 2017-2023



Source: GAO analysis of data from FPS's Modified Infrastructure Survey Tool. | GAO-24-107137

Note: Implementation status is based on recommendations where FPS documented the date of a facility security committee's approval in its system. "Other" includes recommendations that FPS replaced with alternatives and recommendations that did not require a facility security committee response. "Closed not implemented" includes FPS records where no action was taken to implement a recommended countermeasure at a federal facility.

In the discussion groups we held for our 2023 report, participants identified several reasons why a facility security committee may not respond to an FPS recommendation. For example, participants in four discussion groups we held said the ISC's 45-day requirement to approve or reject a recommendation is not a reasonable timeframe to make a decision. Some participants cited the need for additional time to consider expensive and more complex countermeasures. In addition, in the discussion groups, participants stated that cost and feasibility were among the factors that affected decisions to approve and implement FPS recommendations.[16]

[16]GAO-23-105649.

The ISC Is Updating its Annual Questionnaire to Assess the Implementation of FPS-Recommended Countermeasures

In May 2023, we reported that the annual questionnaire the ISC uses to assess compliance with its standards and policies did not include questions on whether federal departments and agencies implemented FPS-recommended countermeasures at federal facilities or whether they accepted risks for countermeasures not implemented, as required by ISC standards.[17] We also reported that ISC did not verify that federal facilities document the acceptance of the risk of not implementing countermeasures. As a result, we recommended that DHS's Cybersecurity and Infrastructure Security Agency improve its oversight of security measures by modifying ISC's compliance and verification process to assess the implementation of FPS's recommended countermeasures. We also recommended that the Cybersecurity and Infrastructure Security Agency modify ISC's compliance and verification process to identify the FPS recommendations for agencies that did not implement recommended countermeasures and did not document the acceptance of the risk.[18] DHS concurred with our recommendations.

In October 2023, ISC officials reported that they are in the process of updating the ISC's annual questionnaire to improve its oversight of members' implementation of recommended countermeasures, including FPS recommendations. According to ISC officials, the questionnaire is being revised and will be published in 2024. In addition, ISC plans to verify the documentation of risk acceptance for countermeasures not implemented for the 10 facilities included in its new compliance verification pilot program.

While the ISC has taken some action, it has not yet fully addressed our recommendations. Completing these efforts to verify selected federal agencies' implementation of recommended countermeasures and their acceptance of risk for unimplemented recommendations may provide ISC a greater level of assurance that facilities are meeting security standards. In addition, improved oversight of recommended countermeasures may provide information to stakeholders and Congress on the extent to which federal facilities have addressed security vulnerabilities and potential threats. Until then, the implementation status of more than 50 percent of FPS's recommended countermeasures will remain unknown and the

[17]GAO-23-105649.

[18]The ISC is chaired by an official from the Cybersecurity and Infrastructure Security Agency via a delegation from the Secretary of Homeland Security.

federal government may not have reasonable assurance that its facilities are secure.

Chairman Peters, Ranking Member Paul, and Members of the Committee, 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, Acting 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 testimony are Roshni Davé (Assistant Director); John F. Miller (Analyst in Charge), Kevin Barsaloux, Derrick Collins, Melanie Diemel, Geoff Hamilton, Shirley Hwang, Alicia Loucks, Minette Richardson, Cristina Toppin, and Elizabeth Wood.