FEDERAL BUILDING SECURITY: EXAMINING THE RISK ASSESSMENT PROCESS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT, AND ACCOUNTABILITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 22, 2022

Serial No. 117–71

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
50–419 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York, Vice Chairman
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MAYRA FLORES, Texas

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT, AND ACCOUNTABILITY

J. LUIS CORREA, California, *Chairman*

DONALD M. PAYNE, JR., New Jersey
DINA TITUS, Nevada
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
PETER MEIJER, Michigan, *Ranking Member*
DAN BISHOP, North Carolina
DIANA HARSHBARGER, Tennessee
JOHN KATKO, New York *(ex officio)*

LISA CANINI, *Subcommittee Staff Director*
ERIC HEIGHBERGER, *Minority Subcommittee Staff Director*
AARON GREENE, *Subcommittee Clerk*

CONTENTS

FEDERAL BUILDING SECURITY: EXAMINING THE RISK ASSESSMENT PROCESS

Thursday, September 22, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT,
AND ACCOUNTABILITY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:11 a.m., in room 310, Cannon House Office Building, Hon. J. Luis Correa (Chairman of the subcommittee) presiding.

Present: Representatives Correa, Payne, Titus, Torres, Meijer, Bishop, and Harshbarger.

Mr. CORREA. Welcome to the Subcommittee on Management, Oversight, and Accountability. I understand our Ranking Member is OK with us proceeding, and he is on his way. I know there is a lot of contradicting messages this morning. We are supposed to be on the floor or in committee or both or neither.

The Subcommittee on Oversight, Management, and Accountability will now come to order. Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning. I want to thank everyone for being here today and for joining us to discuss this most important topic of Federal building security. Protection to facilities, employees, and visitors is a very important part of the Department of Homeland Security's day-to-day work.

As all of you know, tensions have risen recently in response to the FBI's raid on Mar-a-Lago, the passage of the Historic Inflation Reduction Act. We all have seen a rise in threats directed toward Federal employees and Federal office buildings.

Just last month, an armed man attempted to, with violence, gain entrance to an FBI office in Cincinnati. Less well-known are the increasingly threatening language that has been directed to IRS employees and those working to preserve Government documents at the National Archives and Records Administration.

While not typical, though as high-security facilities, these are the Government buildings, and the men and women who work there and visit them every day are now facing new security risks.

With threats to Federal facilities on the rise, we look to the first front lines of defense, the Department of Homeland Security's Federal Protective Service, also known as FPS.

FPS ensures that more than 9,500 Federally-owned and -operated buildings across the country are safe and secure, from Govern-

ment agency headquarters here in Washington, DC, to rural courthouses and field offices across the country, across the 50 States.

If you have ever visited a Federally-owned building, you have noticed thousands of FPS officers and contract guards providing onsite security. But FSP's—I should say FPS's—role extends beyond the guards posted at entrances and exits.

FPS also helps Government agencies prepare for and prevent any security risks that result from a changing threat environment or aging infrastructures.

FPS performs facility security assessments for all Federally-owned buildings and lease buildings and makes recommendations for improvements to ensure that buildings meet required security standards.

These facility assessments and recommendations are very important to ensure that security protocols keep up with the types of threats we are seeing on a day-to-day basis.

The suggested recommendations can range from replacing security cameras and alarms to updating security guidances and policies.

However, despite the good coordination between FPS and other Government agencies, all too often, these recommendations go unimplemented, leaving huge gaps in our security systems.

According to the Government Accountability Office, or GAO, customer agencies have described FPS's facility security assessments as comprehensive, timely, and useful. But they have rejected about 70 percent of FPS's recommendations.

So, again, good recommendations, awesome, but 70 percent of the time, not heeded to.

GAO found that a variety of factors result in the majority of FPS's recommendations not being implemented, including incomplete information and, of course, lack of proper funding.

We can and we should do better in mitigating the risks to facilities, Federal employees, and citizens that visit those buildings.

Today we will have the opportunity to hear more about interagency cooperation that goes into developing building security standards as well as the challenges meeting those standards.

With that, I thank you again for joining us today, our witnesses and other guests.

[The statement of Chairman Correa follows:]

STATEMENT OF CHAIRMAN J. LUIS CORREA

SEPTEMBER 22, 2022

The protection of Federal facilities, employees, and visitors is a critical part of the Department of Homeland Security's day-to-day work. Recently, the importance of this mission has come into stark focus. As tensions have risen in response to the FBI's raid on Mar-a-Lago and the passage of the historic Inflation Reduction Act, we have also seen a rise in the threats directed toward Federal employees and their office buildings.

Just last month an armed man attempted to violently gain entrance to an FBI office in Cincinnati. But perhaps less well-known is the increasingly threatening language that has been directed at IRS employees and those working to preserve Government documents at the National Archives and Records Administration. While not typically thought of as high-security facilities, these Government office buildings, and the men and women who work and visit them every day, are now facing new security risks.

With threats to Federal facilities on the rise, we look to the first line of defense, the Department of Homeland Security's Federal Protective Service, also known as FPS. FPS ensures that over 9,500 Federally-owned and -operated buildings across the country are safe and secure, from Government agency headquarters here in Washington, DC to rural courthouses and field offices in all 50 States. If you have ever visited a Federally-owned building, you have undoubtedly passed one of the thousands of FPS officers and contract guards providing on-site security. But FPS's role extends far beyond the guards posted at entrances and exits.

FPS also helps Government agencies prepare for and prevent any security risks that result from a changing threat environment or aging infrastructure. FPS regularly performs facility security assessments for all Federally-owned and -leased property and makes recommendations for improvements to ensure that buildings meet required security standards. These facility assessments and recommendations are incredibly important to ensure that security protocols keep up with the types of threats we're seeing today. The suggested recommendations can range from things like replacing security cameras and alarms to updating security guidance and policies. However, despite generally good coordination between FPS and the other Government agencies it seeks to protect, all too often these recommendations go unimplemented, leaving gaps to be exploited.

According to the Government Accountability Office (GAO), customer agencies have described FPS's facility security assessments as "comprehensive, timely, and useful," but they have rejected about 70 percent of FPS's recommendations. GAO found that a variety of factors result in the majority of FPS's recommendations not being implemented, including incomplete information and insufficient funding.

We can and should be better to mitigate the risks to facilities, Federal employees, and visitors. Today we will have the opportunity to hear more about the interagency cooperation that goes into developing building security standards as well as the challenges meeting those standards.

Mr. CORREA. I will reserve time for our Ranking Member, Mr. Pete Meijer from Michigan, for an opening statement when he gets here.

With that, Members are reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures.

Without objection, Members not on the subcommittee shall be permitted to sit and question the witnesses.

Mr. Meijer, I call on you for an opening statement, sir.

Mr. MEIJER. Thank you, Mr. Chairman, for holding this important hearing today on the security of Federal buildings across the country. I appreciate the subcommittee diving into this topic, and also I am grateful for our witnesses who are here today to shed light on this important issue.

This subcommittee held a hearing focused on the Federal Protective Service's role in June 2019. I think it is important that we follow up on what was learned in that today.

FPS, as an agency, has evolved over time and has experienced multiple transitions within the Department of Homeland Security.

Formerly established by the General Services Administration in 1971, FPS is the primary Federal agency responsible for the protection of all buildings, grounds, and property owned, occupied, or secured by the Federal Government.

This is obviously an enormous responsibility for an agency that often goes unnoticed and taken for granted. FPS employs 1,300 Federal staff, approximately 944 of whom are law enforcement specialists, criminal investigators, or canine handlers, all of whom trained at the Federal Law Enforcement Training Center, or FLETC.

In addition, FPS heavily relies on more than 15,000 contract guard staff, called protective service officers, or PSOs, to conduct security screenings at more than 9,000 Federal buildings across the country.

PSOs are the backbone of the FPS operation, and without the help of these contract guards, FPS would not be able to carry out its mission.

The protection of our Federal buildings and properties is of utmost significance. Unfortunately, violence against the Government and, in turn, against Federal Government buildings, property, and personnel is not out of the norm and has become more prevalent in recent years. It is incredibly disheartening that we must worry about such things, but we must, and, therefore, our conversation today takes on added importance and relevance.

With such an important mission, we need to ensure that FPS has the tools and authorities to operate as efficiently and effectively as possible.

Of note, FPS has been on GAO's, the Government Accountability Office's, high-risk list since 2003, so nearly 20 years. GAO has found that FPS is not assessing risks at Federal facilities in a manner consistent with standards such as the National Infrastructure Protection Plan's Risk Management Framework, as FPS had originally planned.

This is especially worrisome because a failure by FPS could have catastrophic results. The focus of today's hearing on the security assessment process.

FPS provides security assessments and recommendations to every Federal facility it protects in accordance with the Interagency Security Committee standards. This ISC standard, which is housed within CISA's infrastructure security division, collaboratively establishes, polices, monitors compliance, and enhances the security and protection of Federal facilities.

As we hear from our witnesses today, a large majority of the recommendations that come out of those assessments have not yet been implemented which begs the obvious question of why not.

As we hear, I would like to hear their perspectives from the witnesses on the following questions.

No. 1, is FPS positioned correctly within DHS to be the most effective?

No. 2, how does FPS work with CISA, and how collaborative is that relationship?

No. 3, why do such a large majority of FPS security assessment recommendations go unimplemented, and in turn, is there a better way we can facilitate this process?

No. 4, does FPS have the right force structure with most of their work force being contract support?

No. 5, is the fee structure appropriate and effective for the role of FPS today?

Mr. Chairman, I am grateful we are holding this hearing on this sometimes-overlooked agency within DHS. As they play an ever-important role, protecting our Government, we have to take our oversight responsibility here seriously, and I look forward to hearing from our witnesses to determine what actions we can take moving forward. Thank you and I yield back.

[The statement of Ranking Member Meijer follows:]

STATEMENT OF RANKING MEMBER PETER MEIJER

SEPTEMBER 22, 2022

Thank you, Mr. Chairman, for holding this important hearing today on the security of Federal buildings across the country. I appreciate the subcommittee diving into this topic and appreciate our witnesses for shedding light on such a critical issue. This subcommittee held a hearing focused on the Federal Protective Service (FPS) in June 2019, and I am happy that we can follow up on that hearing today.

FPS, as an agency, has evolved over time and has experienced multiple transitions within the Department of Homeland Security (DHS). Formally established by General Services Administration in 1971, FPS is the primary Federal agency responsible for the protection of all buildings, grounds, and property owned, occupied, or secured by the Federal Government. This is an enormous responsibility for an agency that often goes unnoticed and taken for granted.

FPS employs 1,300 Federal staff. Approximately 944 of those employees are law enforcement specialists, criminal investigators, and canine handlers—all of whom are trained at the Federal Law Enforcement Training Center, or FLETC. In addition, FPS heavily relies upon more than 15,000 contract guard staff, called Protective Security Officers, or PSOs, to conduct security screenings at more than 9,000 Federal facilities across the country. PSOs are the backbone of the FPS operation. Without the help of these contract guards, FPS would not be able to carry out its mission.

The protection of our Federal buildings and property is of the utmost importance. Unfortunately, violence against the Government and, in turn, against Federal buildings, property, and personnel, is not out of the norm and has become even more prevalent in recent years. It is disheartening that we must worry about such things, but we must, and therefore our conversation today takes on added importance and relevance.

With such an important mission, we need to ensure that FPS has the tools and authorities to operate as efficiently and effectively as possible. Of note, FPS has been on GAO's "High Risk" list since 2003. GAO has found that FPS, "is not assessing risks at Federal facilities in a manner consistent with standards such as the National Infrastructure Protection Plan's risk management framework, as FPS originally planned." This is especially worrisome since a failure by FPS could have catastrophic results.

The focus of today's hearing is on the security assessment process. FPS provides security assessments and recommendations to every Federal Facility it protects in accordance with the Interagency Security Committee (ISC) standards. The ISC, housed within CISA's infrastructure security division, collaboratively establishes policies, monitors compliance, and enhances the security and protection of Federal Facilities.

As we will hear from witnesses today, a very large majority of the recommendations that come out of these assessments are not implemented, which begs the obvious question, "why not?"

As we hear from our witnesses today, I would like to hear their perspectives on the following questions:

- Is FPS positioned correctly within DHS to be the most effective?
- How does FPS work with CISA, and how collaborative is that relationship?
- Why do such a large majority of FPS security assessment recommendations not get implemented—and in turn, is there a better way to run this process?
- Does FPS have the right force structure—with most of their workforce being contract support?
- And finally, is the fee structure appropriate and effective?

Mr. Chairman, thank you again for holding this hearing today. This sometimes-overlooked agency within DHS plays an ever-increasing and important role within the Federal Government. I take our oversight responsibility very seriously and look forward to hearing from our witnesses to determine what actions we can take moving forward.

Mr. CORREA. Thank you, Mr. Meijer. Other Members are reminded that statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

SEPTEMBER 22, 2022

We are here today to discuss how the Department of Homeland Security assesses and manages the security risks of the many Federal buildings it is tasked with protecting. I would like to thank Chairman Correa and Ranking Member Meijer for holding today's hearing on this very timely and important topic. I would also like to thank the Federal Protective Service (FPS) workforce for their hard work and service to this country.

During the last few years, when many employees were working at home during the pandemic, FPS was still on the front lines ensuring the safety and security of Federal employees and facilities. FPS is charged with protecting approximately 9,500 Federal buildings, spread across the country, as well as the more than 1.4 million employees, visitors, and customers that enter those buildings each day. Unfortunately, former President Donald Trump's anti-Government rhetoric has encouraged a dangerous surge in threatening language and actions directed toward Federal employees and property.

We have seen what can happen when threats against Federal facilities and employees are not taken seriously. Last year a violent attack on the U.S. Capitol demonstrated that these threats are all too real, and we must be prepared to defend against them. Since that tragic day, we have seen several lone-wolf attacks on Federal facilities outside of our capital region.

FPS's role is to investigate and respond to these threats and to assist Government agencies in preparing for and preventing any security incidents. In addition to providing security guards, FPS also delivers safety awareness trainings, assists with the drafting and implementation of facility-specific emergency plans, and regularly reviews all Federal facilities to identify any potential security gaps. These security reviews are an important resource for assessing whether buildings are equipped to meet the Federal security standards developed by the Interagency Security Committee (ISC).

The ISC, in coordination with FPS, seeks to ensure that all Federal property is adequately protected in the current threat environment—an environment that is ever-evolving. As the nature of threats changes, so must the Federal Government's response. However, all too often roadblocks prevent agencies from implementing FPS's building security recommendations. Better communication is necessary to understand why these barriers exist and what can be done to overcome them without sacrificing the safety of Government workers.

The Government Accountability Office (GAO) has made recommendations aimed at improving the utility of FPS's facility security assessments to help tenant agencies enhance the security of the buildings they occupy. For example, GAO has recommended that FPS improve the cost estimates it provides tenant agencies for recommended security improvements so agencies can make informed decisions about whether and how to implement them. But this communication must go both ways. Tenant agencies should also communicate with FPS when they choose not to implement needed security improvements and explain their reasoning. This cooperation is essential for FPS to effectively carry out its mission.

I look forward to hearing from our witnesses today about how FPS and DHS more broadly can continue to improve the security of Federal facilities.

Mr. CORREA. Now I would like to welcome our panel of witnesses. First, we have Mr. Cline, the principal deputy director for the Federal Protective Service. Mr. Cline has worked with FPS for 20 years, where he coordinates Federal, State, and local officials, to ensure the protection of the buildings, grounds, and properties that are owned, occupied, or secured by the Federal Government.

Mr. Cline previously served 20 years with the U.S. Army Military Police Corps Regimen.

Our second witness, Mr. Scott Breor, associate director for security programs for the Infrastructure Security Division at the Cybersecurity and Infrastructure Security Agency, or CISA.

He helps lead CISA's efforts to secure the Nation's critical infrastructure in coordination with Government and private sectors. Mr. Breor has over 30 years of military and senior executive experience in the U.S. Government.

Our third witness, Ms. Catina Latham, acting director of the physical infrastructure team at the Government Accountability Office, or GAO.

She has worked for GAO for nearly 20 years, where she oversees GAO's work on Federal real property management, including facility security and personal assets.

Without objection, the witnesses' full statements will be inserted into the record, and I now ask each witness to summarize his or her statement in 5 minutes, beginning with Deputy Director Cline. Welcome, sir.

STATEMENT OF RICHARD "KRIS" CLINE, PRINCIPAL DEPUTY DIRECTOR, FEDERAL PROTECTIVE SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CLINE. Good morning, Chairman Correa, Ranking Member Meijer, and distinguished Members of the subcommittee. I am honored to be here today to represent the Federal Protective Service, or FPS, and testify about the essential role we play in protecting Federal employees and facilities. Thank you for the opportunity to raise awareness about the criticality of our mission.

FPS employs nearly 1,000 dedicated law enforcement officers who protect the people and property of the Federal Government. Our services provide protection and deter threats at thousands of Federal facilities across the United States and territories, and protects millions of Federal employees and visitors.

Our highest priority is the safety and security of the more than 1.4 million employees that work in the Federal facilities that we protect. We could not achieve this mission without the dedication and focus of the men and women of the Federal Protective Service.

I firmly believe they are the most dedicated and professional employees in the Federal Government, and it is an honor to represent them here today.

Due to recent acts of violence in communities across the country, our Nation remains in a heightened threat environment. According to the latest DHS-issued National Terrorism Advisory System Bulletin, potential targets include Government facilities and personnel.

There has been an increase in threats toward certain Federal departments and agencies, most notably the Federal Bureau of Investigation, the Internal Revenue Service, and the National Archives and Records Administration.

We have increased our protection efforts at those facilities occupied by these agencies, and remain prepared to detect, prevent, and respond to criminal activities at these locations.

On a given day at a single FPS-protected facility, dozens of our security countermeasures are in place, working together to protect the integrity of buildings and its occupants.

We closely monitor for suspicious activity, while our countermeasure operations ensure our facilities are secure.

Our law enforcement officers and protective security officers are highly trained and prepared to deter attacks, as recently demonstrated at the Chicago and Cincinnati FBI field offices.

Those protective security officers that took action at those locations are typically the first line of defense, and we celebrate their dedication and selfless commitment as we recognize their efforts

this week as part of the National Security Officer Appreciation Week.

From Federal courthouses where high-profile trials take place to daycare centers in Federal facilities where we protect the most innocent, FPS has, time and time again, proven that we are a dynamic, dedicated law enforcement agency.

Additionally, FPS directly protects 233 Congressional district offices that are located in 176 buildings in the FPS protection portfolio.

While we have responsibility for protection efforts at these facilities, we work closely and have strong relationships with the United States Capitol Police and the House and Senate Sergeant at Arms staff to ensure safety of all Members.

Established over 50 years ago, FPS has made remarkable progress as an organization and as the integral part of the Department of Homeland Security's mission to safeguard the American people.

Our law enforcement officers have saved lives by administering life-saving medical treatment, confiscating dangerous weapons, diligently conducting year-long investigations, and even being injured in the line of duty protecting Federal employees and visitors.

Our officers were among those who responded to the all-hands law enforcement call on January 6, 2021, and helped secure the Capitol.

Simply put, FPS has been extremely successful in answering the call to defend and protect the very institutions that allow our Government to function and our country to flourish.

I sincerely appreciate the subcommittee holding this important hearing, and for inviting me to testify on FPS's important role, and I would be pleased to answer and questions you may have. Thank you.

[The prepared statement of Mr. Cline follows:]

PREPARED STATEMENT OF RICHARD "KRIS" CLINE

SEPTEMBER 22, 2022

INTRODUCTION

Chairman Correa, Ranking Member Meijer, and Members of the subcommittee. Thank you for the opportunity to testify today on behalf of the U.S. Department of Homeland Security's (DHS) Federal Protective Service (FPS) regarding FPS's critical mission to protect and secure U.S. Government Federal facilities.

My name is Richard K. Cline and I serve as FPS's principal deputy director, a position that I have held since August 2017. In this role I work closely with the FPS director, Eric Patterson, to manage FPS's diverse and nationally-dispersed workforce and coordinate with Federal, State, and local public officials to ensure the protection of the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government, as well as the persons on those properties. Prior to serving as the FPS principal deputy director, I served several years as FPS's deputy director for operations, a role that allowed me to gain familiarity and experience with FPS's operations across the Nation. I am pleased to be joined by the Government Accountability Office, with whom our agency maintains a very positive relationship, as well as the Cybersecurity and Infrastructure Security Agency (CISA). FPS works collaboratively with CISA's Interagency Security Committee (ISC) and leverages the great work of the ISC in many of our programs, including our Facility Security Assessment process, conducted through our ISC-certified Modified Infrastructure Survey Tool, as well as our ISC-certified training curricula at our national training academy at the Federal Law Enforcement Training Centers (FLETC).

Last year, FPS celebrated its 50th anniversary as an agency. Since its inception in 1971, FPS has protected people and property in the Federal Government by identifying and mitigating vulnerabilities through risk assessments, law enforcement, intelligence analysis, and security countermeasures.

FPS personnel are located in every U.S. State and territory, charged to protect over 9,000 Federal facilities and more than 1.4 million people who work, visit, or conduct business at these facilities. Our mission serves 66 different Federal agencies each day, ensuring safe work environments for Federal employees performing the essential duties that impact the day-to-day lives of Americans. FPS continually adapts to meet threats, working with our Federal, State, and local partners to ensure complete security coverage and efficient communication to protect people and property. We have well-established procedures in place to address threats to Federal property and have been successful in mitigating these threats.

While our core mission has remained the same during our 51 years, we have made remarkable progress in our capabilities. FPS has leveraged technology, training, and partnerships to detect and deter crime before it happens. With expertise in all aspects of policing and physical security, FPS is a recognized, award-winning leader in facility protection. We also realize that as our capabilities grow, so too do those of our adversaries.

Though our organization might not be a household name, we often assist in some of the country's most urgent and critical responses and operations, from protecting Federal facilities at the U.S.-Mexico border to responding to active shooters and even assisting the U.S. Capitol Police on January 6, 2021. This level of dedication to our country's security comes with the highest of costs. Each day, our law enforcement officers risk their lives to protect and secure the Government of this great Nation.

In its history, 7 sworn FPS officers and 3 Protective Security Officers (PSO), who are our contracted security guard force, have died in the performance of their duties. This serves as a stark reminder that the men and women who wear the FPS uniform are prepared to sacrifice all in service to our country and Government, and we must ensure they are supported in every way possible to respond to and prevent the threats of our Nation's people, property, and institutions.

FPS HISTORY

In 1790, 6 "night watchmen" were hired to protect Government buildings in the newly-designated Nation's capital that became Washington, DC. Over time, the network of security guards evolved and was known as the U.S. Special Police. In 1971, the "Federal Protective Service" was established. FPS was transferred to the Department of Homeland Security (DHS) on March 1, 2003, pursuant to the Homeland Security Act of 2002 (6 U.S.C. §§ 101 et. seq) in recognition of the role that it plays in securing the homeland. FPS now resides under the Management Directorate in DHS Headquarters. Headquartered in Washington, DC, FPS is organized through three zones and 11 regions for mission execution.

FPS WORKFORCE

Our law enforcement personnel, made up of over 1,000 men and women stationed across the country, are physical security experts and sworn Federal law enforcement officers, trained with cutting-edge technologies and techniques that allow us to remain an effective and responsive force. These law enforcement officers perform a variety of critical functions, including conducting comprehensive security assessments to identify vulnerabilities at Federal facilities, developing and implementing protective countermeasures, providing uniformed police response and investigative follow-up to crimes and threats, and other law enforcement activities in support of our mission. FPS's law enforcement mission involves responding to a range of threats and incidents, including the recent attack at the Federal Bureau of Investigation facility in Cincinnati, Ohio, where our PSOs prevented an assailant from gaining access to the facility. FPS law enforcement personnel maintain regular communication with Federal, State, and local law enforcement entities across all regions and have open exchanges of information.

Within FPS, nearly 400 mission support staff are responsible for a myriad of important tasks, including outreach and engagement with critical external stakeholders (e.g., Congress and the Federal Executive Boards); human capital management; finance, budgeting, and security officer contract oversight; and security training and law enforcement.

FPS, through contracts with commercial security vendors, relies on approximately 15,000 PSOs to assist in the protection of Federal facilities. Some of FPS's PSOs service providers (i.e., contractors) are experiencing staffing shortages in the post-

pandemic environment. Ultimately, each contractor is responsible for planning and appropriately staffing its contract with a sufficient number of PSOs, and FPS Contracting Officers are currently working with contractors experiencing staffing shortages to ensure that they will provide a level of staffing that will meet all contractual requirements. Despite the challenge of coverage, our PSOs are often the front line of FPS and are in daily contact with our Federal facility customers and visitors. They, too, put themselves at risk to accomplish our mission. FPS has lost three PSOs in the line of duty since 2015, all of whom were tragically killed protecting Federal facilities and employees.

FPS AUTHORITIES

FPS has broad law enforcement authorities and jurisdiction to prevent, investigate, mitigate, and defeat threats to Federal property and people on Federal property. Section 1706 of the Homeland Security Act, 40 U.S. Code § 1315, grants FPS traditional police powers, including the authority to enforce Federal law and to make arrests. In certain circumstances, FPS has the ability to enter into agreements and utilize other Federal, State, and local law enforcement authorities for purposes of protecting Federal property. For example, in the District of Colombia (DC), FPS has an agreement with the Metropolitian Police Department allowing FPS to enforce the DC penal code 300 feet from listed Federal facilities and expanded distances from St. Elizabeths campus and the Nebraska Avenue Complex.

FPS FUNDING STRUCTURE

FPS is completely funded by the fees it charges Federal departments and agencies to execute its mission and does not receive a direct appropriation. We have established a risk-based revenue model to align basic security assessments with the security work that FPS performs. This method employs statistical analysis of operational workload data at each building to understand the key drivers of FPS's security costs. FPS uses a three-factor model to determine that operational workload data. The first factor is the total volume of service calls made to FPS and security alarm activations from each building within the portfolio. The second factor is the total number of times an emergency responder is dispatched to incidents for each FPS-protected facility. The final model factor is the total quantity of PSO posts set at each facility. FPS uses this three-factor model to determine the basic security assessments for each customer agency. This approach is equitable for assessing basic security fees because it reflects FPS's historical security workload data for each building.

FPS OPERATIONS

FPS ensures safety through five vital functions:

- Facility threat and security assessments through Facility Security Assessments (FSAs);
- On-site facility and event security through FPS's Countermeasures and PSO Program;
- Intelligence gathering and sharing through FPS's Government Facility Sector program;
- Criminal investigation through law enforcement certified Special Agents and Inspectors; and
- Incident and emergency response through deployment of law enforcement and FPS's Rapid Protection Force in times of need.

Our personnel work every single day, including during holidays and natural disasters. This means that every day of the year, FPS employees could be fulfilling any of the following duties:

- Conducting security assessments of Federal facilities to identify risks;
- Designing, installing, and maintaining security countermeasures to mitigate risks;
- Providing a visible law enforcement response and presence;
- Overseeing contract security guards who conduct access control and security screening;
- Performing background suitability checks for FPS contract personnel;
- Conducting criminal investigations, including threats to Federal employees and facilities;
- Monitoring security alarms via centralized communication centers;
- Integrating and sharing criminal intelligence for risk-informed decision making;
- Providing security during Federal Emergency Management Agency Stafford Act deployments, National Special Security Events and Special Event Activity Rating events;

- Leading special operations, including canine explosive detection operations; and
- Training Federal employees in active shooter response, crime prevention, and occupant emergency planning.

FSAs represent a cornerstone of FPS's approach to comprehensive security. Our inspectors are rigorously trained to identify potential facility vulnerabilities. Working with security specialists, countermeasure experts, and FPS leadership, our inspectors provide these detailed reports to facility tenants as our FPS recommendations for adequate building security and coverage. FPS designed and implemented an award-winning computer program, Modified Infrastructure Survey Tool (MIST), to further evaluate and identify potential threats at FPS-secured locations. Using both the institutional knowledge of our inspectors with the high-performance capabilities of MIST means that our FSAs are a superior resource for providing our customers with the best possible security enhancement suggestions.

In 2021, at the behest of Chairman Correa, the Government Accountability Office (GAO) conducted and released a report that examined our stakeholders' perspectives of FPS's performance. The report, which revealed that our stakeholders are largely satisfied with our services, provided recommendations to our FSA cost estimation process. Since then, FPS has implemented changes to its FSA reports to better detail the accuracy of cost estimates for recommended security measures. Additionally, we have begun providing new training and additional resources to our staff to enable them to develop countermeasure cost estimates that are more accurate and detailed.

FPS ACCOMPLISHMENTS IN 2021

For FPS, 2021 was a landmark year that focused on: Cutting-edge innovations, collaborations with other law enforcement agencies, and, most importantly, a committed workforce which excelled and achieved unprecedented successes in our organization's history. Faced with the challenges of the global COVID–19 pandemic, FPS has never wavered in our mission readiness. We undertook a record number of criminal and threat investigations, achieved breakthroughs in countermeasure capabilities, and led the Federal law enforcement community in establishing a comprehensive public order policing policy. While a comprehensive list of our accomplishments is too numerous to account for here, below are some notable highlights:

- Last year, FPS made 1,148 arrests and citations issued under its governing authorities and criminal statutes, ensuring the safety of those employees and visitors of FPS-protected facilities while also preserving the Constitutional rights of American citizens.
- Equipped with a cadre of Special Agents, FPS opened nearly 400 cases and investigated 276 threats to Federal property and persons thereon in 2021. Those investigations have led to at least 7 convictions, 25 arrests, and 16 citations for Federal, State, and municipal penal code violations, U.S. District Court Notices of Violations, and criminal charges under Title 18 of the U.S. Code.
- In 2021, FPS made 4,625 recommendations to add or upgrade countermeasures at FPS-protected Federal facilities, including assisting U.S. Marshals at U.S. Courthouses where several nationally-prominent trials were held, such as the trial of two men in Michigan charged with and convicted of plotting to kidnap the Michigan Governor.
- Last year, FPS conducted 1,979 FSAs, to help our stakeholders identify security requirements.
- FPS has had a significant role in DHS's Countering Unmanned Aircraft Systems program, a cutting-edge countermeasure technology that monitors the skies of FPS-protected facilities for unauthorized unmanned aircraft, just one example of how FPS evolves to meet emerging threats.
- FPS's 70 Explosive Detection Canine Teams provide specialty services throughout the homeland, sweeping buildings, vehicles, parking lots, and other structures for potential explosives. Their presence not only helps locate potential explosives, but also serves as a deterrent to criminals. In 2021, FPS's Canine Teams made 103,512 total sweeps, including 28,258 building sweeps and 75,254 vehicle sweeps.
- One of FPS's newest divisions, the Cyber-Physical Division, completed 19 Cyber Security Assessments at 19 separate, large-scale Federal facilities, resulting in the identification and remediation of 61 cyber vulnerabilities to Federal systems.
- More than a dozen FPS officers assisted the U.S. Capitol Police to secure the U.S. Capitol on January 6, 2021.
- FPS developed and issued a Public Order Policing policy directive—a first for the agency and the Department—that clearly outlines instructions on how Law

Enforcement Officers should manage and respond to First Amendment-protected activities and other types of crowd management events.

CONCLUSION

FPS continues to demonstrate that we are more than capable of deterring and responding to any and all threats toward Federal employees, visitors, and facilities.

The FPS mission must be accomplished every day to ensure the continuity of the U.S. Government and our great country. Support from Congress and our stakeholders can help us progress as a law enforcement agency responsible for securing these sacred Governmental institutions.

I am very proud of all that FPS has accomplished in our rich 51-year history, and I know that our talented and committed workforce will always ensure we are ready to meet our mission as it continues to evolve.

I would like to acknowledge and thank the distinguished Members of this subcommittee for allowing me the opportunity to testify today.

I would be pleased to answer your questions.

Mr. CORREA. Thank you. I recognize Mr. Breor to summarize his statement for 5 minutes. Welcome, sir.

STATEMENT OF SCOTT BREOR, ASSOCIATE DIRECTOR OF SECURITY PROGRAMS, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BREOR. Thank you, sir. Chairman Correa, Ranking Member Meijer, Members of the subcommittee, as the associate director for security programs within Cybersecurity and Infrastructure Security Agency's infrastructure security division, I appreciate the opportunity to appear before you today to discuss the Interagency Security Committee's role in the protection of Federal buildings and its efforts to improve preparedness and coordination with interagency partners.

On October 19, 1995, 6 months after the Oklahoma City bombing at the Alfred P. Murrah Federal Building, President Clinton issued Executive Order 12977, creating the Interagency Security Committee, or ISC, to address the quality and effectiveness of physical security requirements of Federal facilities.

Membership of the ISC consists of senior-level executives from 66 Federal departments and agencies. This collective security subject-matter expertise allows the ISC to develop top-tier risk management resources, and to coordinate interagency solutions to problems that cannot be solved by individual departments and agencies alone.

The ISC is a collective forum that carries out its work by, with, and through its members with a primary governance framework of subcommittees and working groups. These working groups, which are provisional, are task-based bodies, established by the ISC, with clear objectives and defined deliverables.

In March 2003, the role of chair transferred from the General Services Administration to DHS. DHS delegated this responsibility to CISA in light of its role to help protect and secure the Nation's critical infrastructure.

CISA stewardship of the ISC ensures its work both supports and leverages State, local, territorial, and Tribal organizations, as well as the private sector, all essential partners as we work to ensure the continued protection of Federal facilities and assets across the Nation and around the world.

Executive Order 12977 gave the ISC three key responsibilities. These include: Establish policies for security in and protection of Federal facilities; develop and evaluate security standards, and a strategy to ensure compliance; and take actions to enhance the quality and effectiveness of security and protection of Federal facilities.

The ISC fulfills these responsibilities through multiple lines of effort, including the risk management process standard. The risk management process standard provides an integrated, single source, physical security countermeasures and guidance on countermeasure customization for all nonmilitary Federal facilities.

ISC members created the risk management process standard to provide a common method for all Federal facility security stakeholders to guide risk assessments in a standardized way and to help facility owners identify the levels of protection needed to mitigate that risk.

Further, the ISC validates member risk assessment tools and training programs as meeting the risk management process standard. This helps build individual and organizational capability to successfully implement ISC guidance in conducting these assessments.

FPS uses a risk assessment tool that has been validated by the ISC, the Modified Infrastructure Survey Tool. Additionally, FPS's Physical Security Training Program, located at the Federal Law Enforcement Training Center, has similarly been validated by the ISC.

This training program trains FPS personnel on how to conduct a risk assessment using their validated Modified Infrastructure Survey Tool.

Two of the main drivers of threats to Federal facilities are targeted violence and terrorism. As noted in the most recent DHS National Terrorism Advisory System Bulletin, these threats are becoming more varied and complex. Combating them is and will remain a top priority of DHS.

DHS is committed to using every resource available to prevent, detect, and mitigate threats of violence directed at Federal facilities.

Thank you again for the opportunity to appear before you today, and for this committee's continued support of CISA and the Department. I look forward to continuing to work closely with you and other Members of Congress to keep our Federal facilities and those who work at and visit them safe and secure.

[The prepared statement of Mr. Breor follows:]

PREPARED STATEMENT OF SCOTT BREOR

SEPTEMBER 22, 2022

INTRODUCTION

Chairman Correa, Ranking Member Meijer, and Members of the subcommittee, my name is Scott Breor, and I am the associate director for security programs within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) Infrastructure Security Division (ISD). I appreciate the opportunity to appear before you today to discuss the DHS's Interagency Security Committee's (ISC) role in the protection of Federal buildings and its efforts to improve preparedness, in coordination with interagency partners.

THE INTERAGENCY SECURITY COMMITTEE AND ITS ROLE IN THE PROTECTION OF FEDERAL FACILITIES

The ISC was created in the wake of the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. The attack on that Federal facility served as a national tragedy with the loss of 168 lives, including 19 children. To this day, the Oklahoma City attack remains the deadliest domestic terrorist attack on American soil in our history.

Following the Oklahoma City bombing, President Bill Clinton issued Executive Order (EO) 12977 to "enhance the quality and effectiveness of security in and the protection of buildings and nonmilitary Federal facilities in the United States," and to create the ISC. DHS has chaired the ISC since March 2003, when, pursuant to EO 13286, the role of chair transferred from the General Services Administration (GSA) to DHS. DHS delegated this responsibility to CISA as a result of its role as the Nation's risk advisor and its task to help secure critical infrastructure. CISA provides the leadership, management, and compliance monitoring necessary to meet the requirements of EO 12977. CISA's stewardship of the ISC ensures its work both supports and leverages State, local, territorial, and Tribal organizations, as well as the private sector, all of whom are essential partners as we work to ensure the continued protection of Federal facilities and assets across the Nation and around the world.

ROLE OF THE INTERAGENCY SECURITY COMMITTEE IN FEDERAL FACILITY SECURITY

When the ISC was created in 1995, it consisted of the 21 members outlined in EO 12977. Today, the ISC includes 66 members. In addition to Executive branch agencies, the ISC includes representatives from outside the Executive branch such as the United States Capitol Police and the Administrative Office of the United States Courts. Membership consists of departments and agencies whose headquarters are both inside and outside the National Capital Region. This collective security subject-matter expertise allows the ISC to develop top-tier risk management resources and to coordinate interagency solutions to problems that cannot be solved by individual departments and agencies alone.

The ISC is a collaborative forum that carries out its work by, with, and through its members within a primary governance framework of subcommittees and working groups. The ISC's eight standing subcommittees guide the development of ISC policies and strategic initiatives. Additionally, the ISC establishes working groups, which are provisional, task-based bodies with clear objectives and defined deliverables.

EO 12977 gave the ISC three key responsibilities. These include:

- Establish policies for security in, and protection of, Federal facilities;
- Develop and evaluate security standards and a strategy to ensure compliance; and
- Take necessary actions to enhance the quality and effectiveness of security and protection of Federal facilities.

The ISC fulfills these responsibilities through multiple lines of effort. The first is the Risk Management Process: An Interagency Security Committee Standard (RMP Standard). The RMP Standard provides an integrated, single source of physical security countermeasures and guidance on countermeasure customization for all nonmilitary Federal facilities. ISC members created the RMP Standard to provide a common method for all Federal facility security stakeholders; specifically owning and leasing organizations, security organizations and the members of departments and agencies that are tenants in Federal facilities; to guide risk assessments of Federal facilities in a standardized way and to help facilities owners identify levels of protection needed to mitigate that risk.

In addition to the core RMP Standard, the ISC produced and issued over 20 other products, including authoritative guidance on planning and response to an active-shooter situation, a standard for prohibited items at Federal facilities, and other best practices and guides. ISC guidance documents are distributed via department and agency member representatives and senior leaders within their organizations. Federal facility security stakeholders can also download the documents from the ISC web presence at CISA.gov. Each organization uses best practice documents and guides as a means to enhance the security of and protection of Federal facilities, and those who visit or occupy them. A sample of these products include:

- Security Convergence: Achieving Integrated Security: An Interagency Security Committee Best Practice;
- Protecting Against the Threat of Unmanned Aircraft Systems (UAS): An Interagency Security Committee Best Practice;
- Facility Access Control: An Interagency Security Committee Best Practice;

- Violence in the Federal Workplace: A Guide for Prevention and Response;
- Facility Security Plan: An Interagency Security Committee Guide; and
- Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide.

ISC guidance is designed to be scalable and tailorable to the unique security environment and site-specific needs of the diverse membership of the ISC. Further, the ISC validates member risk assessment tools and training programs as meeting the RMP Standard. This helps build individual and organizational capability to successfully implement ISC guidance.

The ISC also monitors compliance with its policies and standards at the organizational and facility level. This includes providing Federal facility stakeholders with the means to measure, report, and analyze compliance against a set of benchmarks using a web-based platform. The resulting data and analyses help departments and agencies focus their efforts and resources while providing feedback to the strategic direction of the ISC's work. Examples of areas where this valuable information has informed action include refining policy, developing training and other capacity-building efforts, and developing automated support tools. The results of ISC compliance findings are briefed to the ISC Chair, and also made available to the relevant ISC member departments and agencies, to ensure necessary corrective actions are taken to enhance compliance with ISC policies and standards.

ISC PARTNERSHIP WITH THE FEDERAL PROTECTIVE SERVICE

CISA, through its stewardship of the ISC, works with partners across Government and the private sector to ensure our Nation's Federal facilities are protected against the threats of today. Two of the main drivers of threats to Federal facilities are targeted violence and terrorism. As noted in the DHS National Terrorism Advisory System Bulletin, these threats are becoming more dynamic and complex—combatting these threats is and will remain a top priority for DHS. Within DHS, our partners at the Federal Protective Service (FPS) play a key role on the ISC. FPS actively contributes to 7 of the ISC's 8 standing subcommittees and all 3 operating working groups. The FPS also provides valuable leadership, chairing 2 of the 8 subcommittees and 1 of the 3 working groups.

In addition to contributing to the collective work of the ISC, FPS provides security for facilities under GSA's jurisdiction, custody, or control as well as numerous non-GSA Federal properties throughout the country. As part of this responsibility, FPS conducts risk assessments to identify risk(s) and recommended security countermeasures to mitigate corresponding risk(s). In conducting these assessments, FPS uses a risk assessment tool that has been validated by the ISC, the Modified Infrastructure Survey Tool. Additionally, FPS's Physical Security Training Program located at the Federal Law Enforcement Training Centers has similarly been validated by the ISC. This training program trains FPS personnel on how to conduct a risk assessment using their validated Modified Infrastructure Survey Tool (MIST).

CONCLUSION

DHS is committed to using every resource available to prevent, detect, and mitigate threats of violence directed at Federal facilities. Securing and protecting Federal facilities is both a DHS-wide and an interagency effort.

Thank you again for the opportunity to appear before you today, and for this committee's continued support of CISA, the Department, and our efforts. I look forward to continuing to work closely with you and other Members of Congress to keep our Federal facilities, and those who work at and visit them, safe and secure.

Mr. CORREA. Thank you for your testimony, and I now recognize Ms. Latham to summarize her statements in 5 minutes or less. Welcome.

STATEMENT OF CATINA B. LATHAM, DIRECTOR OF THE PHYSICAL INFRASTRUCTURE TEAM (ACTING), U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Ms. LATHAM. Thank you. Good morning. Chairman Correa——

Mr. CORREA. Good morning.

Ms. LATHAM [continuing]. Ranking Member Meijer, and Members of the subcommittee, thank you for the opportunity to discuss the Federal Protective Service's security risk assessments.

As you have mentioned, we have designated Federal real property management as a high-risk area since 2003, in part, because of the physical security challenges at Federal facilities.

My statement today will focus on our prior and on-going work on FPS. First, I will cover the stakeholders' views on FPS facility assessments and the implementation status of FPS security recommendations.

Next, I will discuss the preliminary observations of FPS law enforcement deployments.

First, we reported in June 2021 that stakeholders were generally satisfied with FPS security assessment process. However, many of them expressed concern with the cost estimates FPS provided in these reports, as they lacked important information that could help agencies make decisions.

Stakeholders reported their concerns about the cost estimates may discourage them from implementing security measures intended to reduce the security threats.

In that report, we recommended that the director of FPS ensure that facility security assessments document both the assumption and sources used to develop the cost estimates for each recommended security measure.

As of August 2022, FPS had taken steps to address our recommendations, in part, by updating its directive and manual for conducting these assessments. We are now in the process of analyzing if FPS actions are fully responsive to our recommendations.

Next, FPS data indicate that security recommendations are generally not implemented, as the Chairman mentioned. Our analysis show that between fiscal years 2017 and 2021, FPS made more than 25,000 security recommendations at nearly 5,000 Federal facilities.

Now, these recommendations range from addressing physical vulnerabilities to ensuring policy or guidance documents are current.

Furthermore, FPS data shows it did not receive a decision as to whether agencies approved or rejected more than half of the 25,000 security recommendations.

This data also shows an agency's approval of a recommendation does not necessarily mean it will be implemented. Of about the 6,800 of the approved recommendations, only about 22 percent have been implemented as of September 2022.

FPS officials also noted that some recommendations stay open for years, as it can take time to secure the funding and implement some of the more costly recommended security measures.

In our on-going work, we will explore and identify factors that influence agencies' decisions to approve or reject security recommendations, and we will also look at why FPS is not receiving information on those decisions. We expect to report on this work in early 2023.

In addition to conducting facility security assessments, FPS provides law enforcement support to other Federal agencies. Preliminary observations from our on-going work shows that the number of days FPS has deployed law enforcement officers has increased since fiscal year 2020.

These officers are deployed to augment security at FPS-protected facilities to support other agencies' homeland security operations.

FPS deployments, for example, have helped in securing Federal facilities during protests and housing units for migrants in the Southwest Border region.

As a final point, staffing is also an important consideration as FPS continues to have shortages. In June 2010, when FPS was in the Cybersecurity and Infrastructure Security Agency, we reported that FPS had difficulty obtaining needed staff.

FPS had not filled 21 percent of its authorized positions, including about 200 law enforcement positions.

We are currently conducting work on these changes since FPS moved to the management directorate and how they are collaborating to address FPS staffing shortages. We expect to release an issue on this work by the end of 2022.

Chairman Correa, Ranking Member Meijer, and Members of the subcommittee, this concludes my statement. I am happy to answer your questions.

[The prepared statement of Ms. Latham follows:]

PREPARED STATEMENT OF CATINA B. LATHAM

THURSDAY, SEPTEMBER 22, 2022

GAO HIGHLIGHTS

Highlights of GAO–22–106177, a testimony before the Subcommittee on Oversight, Management, and Accountability, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

Over 1 million Federal employees and visitors depend on FPS to provide security and protection at more than 9,000 facilities across the country. FPS assesses these facilities to identify security risks and then recommends security measures. In addition to this work, FPS provides law enforcement services on a short-term basis or in specific situations for individual agencies.

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

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

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

FEDERAL PROTECTIVE SERVICE.—MANY APPROVED SECURITY RECOMMENDATIONS WERE NOT IMPLEMENTED AND PRELIMINARY WORK SUGGESTS LAW ENFORCEMENT DEPLOYMENTS HAVE INCREASED

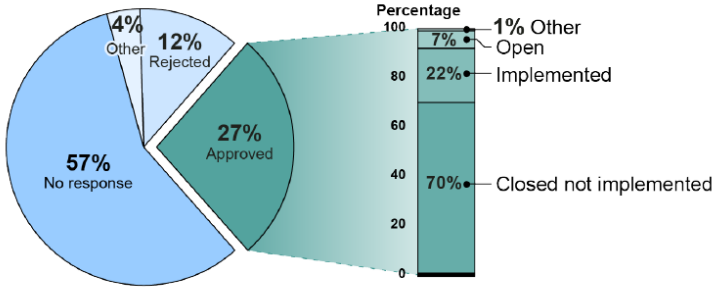
What GAO Found

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

In on-going work, GAO found it was unclear if agencies were still in the process of deciding whether to approve most of FPS's recommendations or if they had ac-

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

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



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

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

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

Chairman Correa, Ranking Member Meijer, and Members of the subcommittee: Thank you for the opportunity to discuss our work on security services provided by the Department of Homeland Security's (DHS) Federal Protective Service (FPS). FPS plays an important role in ensuring the day-to-day security of over 1 million Federal employees and visitors at more than 9,000 Federal facilities. The General Services Administration (GSA) serves as the landlord for most of these facilities, with Federal agencies renting space from GSA and thus serving as tenants. FPS provides security and protection at these facilities, in part, by conducting facility security assessments to identify security risks and recommending security measures for agencies to implement to address or mitigate these risks. Agencies' implementation of the recommended security measures is an important step in protecting employees, visitors, and facilities.

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

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

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

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

This statement is based in part on our report issued in June 2021 about stakeholders' perspectives on FPS's performance of key activities, including conducting facility security assessments. It is also based on our on-going work related to FPS security recommendations and the impact of FPS's recent move to the Management Directorate within DHS.[2]

In conducting our prior work related to FPS's security assessments, we held 6 discussion groups with stakeholders from 27 randomly selected facilities where FPS provided services. The views of these stakeholders are not representative, but collectively provided insight into stakeholders' satisfaction with how FPS was performing key activities. We also compared FPS's facility security assessment reports to criteria in GAO's Cost Estimating and Assessment Guide.[3] In our current work, we obtained data from FPS's risk assessment tool on recommendations made during fiscal years 2017 through 2021. We analyzed the data to identify the types of recommendations made and the approval and implementation status of the recommendations. We assessed the data against GAO data reliability standards, including reviewing FPS guidance and processes for safeguarding and checking the data for accuracy and completeness. We determined the data were sufficiently reliable for the purposes of describing the type and implementation status of FPS recommendations.

Our work to understand FPS's law enforcement deployments is on-going. We analyzed data on the extent to which FPS law enforcement staff were deployed to support homeland security operations in fiscal year 2020 and fiscal year 2021 as well as data on the extent to which FPS had unstaffed positions as of the end of fiscal year 2021. Additionally, we interviewed officials from FPS, including 5 FPS Regional Directors, to understand how FPS's deployments and staff resources have changed since its move to the Management Directorate in 2019.[4]

We conducted this work in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

Organizational Responsibilities

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

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

In addition to protecting GSA facilities, FPS participates in homeland security activities such as providing law enforcement, security, and emergency-response services during natural disasters and special events.[6] In our January 2019 report and June 2019 testimony on FPS's organizational placement, we reported that FPS's responsibilities grew beyond solely protecting GSA facilities to include homeland security activities when it moved from GSA to DHS's Immigration and Customs Enforce-

---

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

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

[4] We selected directors in the 5 largest regions in terms of FPS's authorized positions in fiscal year 2021.

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

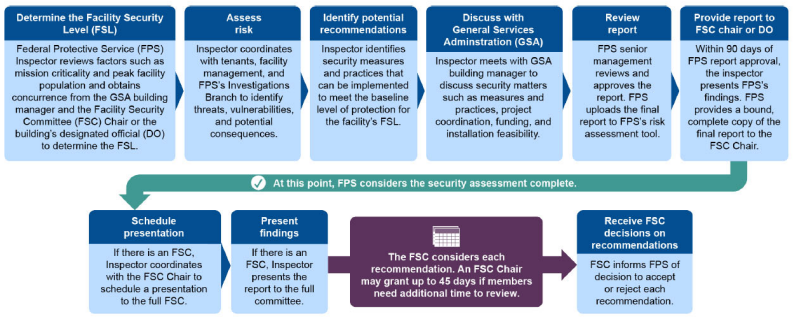
[6] FPS derives its law enforcement authority with respect to the protection of buildings, grounds, and property that are owned, occupied, or secured by the Federal Government, and the persons on the property, from the Secretary of Homeland Security pursuant to 40 U.S.C. § 1315.

ment in March 2003.[7] FPS continued to participate in such activities in each of its subsequent organizational placements in DHS: the National Protection and Programs Directorate (which was later re-designated as the Cybersecurity and Infrastructure Security Agency)[8] and the Management Directorate.[9] FPS transitioned to DHS's Management Directorate—its current placement—in October 2019.[10]

Facility Security Assessments

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

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



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

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

ISC standards require FPS to conduct these assessments every 3 to 5 years, depending on the security level of the facility.[12] FPS tracks scheduling and completion of its assessments for all facilities at all risk levels using data that the inspectors enter into FPS's risk assessment tool (i.e., Modified Infrastructure Survey Tool or MIST). FPS reported that in fiscal years 2017 through 2021 its inspectors completed

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

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

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

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

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

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

100 percent of facility security assessments for high-risk facilities within the required time frame.[13]

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

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

FPS Budget and Staff

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

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

STAKEHOLDERS WERE GENERALLY SATISFIED WITH FPS'S SECURITY ASSESSMENT PROCESS; YET MANY FPS RECOMMENDATIONS WERE NOT IMPLEMENTED

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

In June 2021, we reported that the participants of our discussion groups—tenant agency officials and GSA building managers—generally held positive views about the content of FPS's security assessment reports and FPS's communication about the reports.[15] Participants from all six discussion groups characterized the reports as thorough, comprehensive, timely, and useful. Many participants also expressed satisfaction with FPS's communication of the security assessment results. However, several building manager participants told us that they had not been invited to an FPS presentation of security assessment results. According to the FPS Facility Security Assessment Manual, FPS is to work with the FSC chair to schedule and hold a presentation of the security assessment results to the committee. The FSC chair is responsible for inviting members of the committee to meetings. However, we also reported that many stakeholders expressed concern with the cost estimates FPS provides in its security assessment reports.[16] Participants from all three groups of building managers and one group of tenant agency participants said that FPS's cost estimates are not sufficiently detailed to inform participants' decisions on rec-

---

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

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

[15] GAO–21–464.

[16] GAO–21–464.

ommended security measures and practices.[17] Based on the comments from our discussion group participants, stakeholders' concerns with cost estimates may discourage them from implementing security measures intended to reduce security risks. For example, one building manager participant observed that lack of details about cost estimates caused delays and resulted in unimplemented recommendations.

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

In our June 2021 report, we recommended that the director of FPS ensure that Facility Security Assessment reports document the assumptions and sources used to develop the cost estimate for each recommended security measure.[19] As of August 2022, FPS had taken steps to address our recommendation in part by updating its directive and manual for conducting facility security assessments. We are assessing FPS's actions to determine if they fully address our recommendation.

FPS Data Indicate That Security Recommendations Are Generally Not Implemented

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

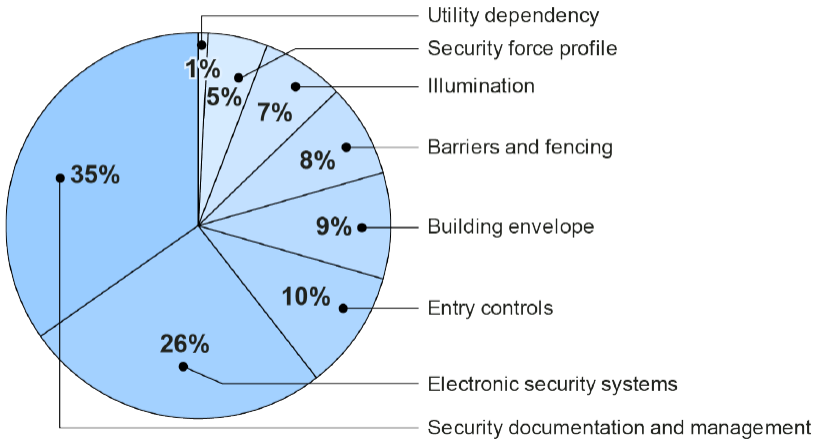
- *Barriers and fencing*.—physical obstacles used to restrict access to facilities. Barriers are fixed or movable objects, such as bollards or spike systems, that are used to mitigate or reduce the impact of a vehicle ramming a building or a checkpoint.
- *Building envelope*.—exterior surface of the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

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

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

[19] GAO–21–464.

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

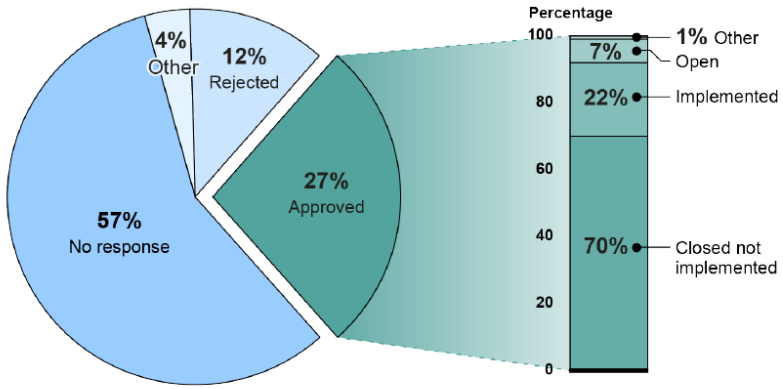


Source: GAO analysis of data from FPS's Modified Infrastructure Survey Tool. | GAO-22-106177

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

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

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



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

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

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

OUR PRELIMINARY WORK SHOWS THAT FPS HAS INCREASED LAW ENFORCEMENT DEPLOYMENTS AND CONTINUES TO FACE STAFFING SHORTAGES

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

FPS officials said that FPS is more involved in other DHS components' homeland security operations since the agency moved from the Cybersecurity and Infrastructure Security Agency to the Management Directorate in October 2019.[22] They said FPS is more involved because the acting under secretary for management has shown support for FPS's facility protection mission and legal authorities, and ensured that DHS components are aware of FPS's role. FPS officials also said that their increased participation in homeland security operations has improved the agency's credibility within DHS; they said this improved credibility has been one of the benefits of moving to the Management Directorate.

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

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

---

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

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

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

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

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

Mr. CORREA. Thank you very much. I want to thank all the witnesses, all of you, for your testimony, and I will remind the subcommittee that each one of us has 5 minutes to question the panel, and I will recognize myself for 5 minutes of questions.

Your testimony, very important. Seventy percent of FPS's recommendations, not implemented. Ms. Latham, you cite a number of factors—budgets. You cited the challenges in the Southern Border. Is this 70 percent nonimplementation something new, or has this been something that has been going on for a number of years? Ms. Latham.

Ms. LATHAM. Thank you for the question. The work that we are doing now, we are certainly going to look further in depth into how long this has been a standing issue of not being implemented.

Some of the reasons, as you mentioned, that we had heard in our prior work was due to not having the cost estimates as I noted. The agencies noted that they needed these cost estimates to just further understand the scale of what is needed to address them.

They also said that they needed the information, for example, if they were in a building that was older and needed——

Mr. CORREA. Let me interrupt you, I only have a couple minutes to ask these questions. But, again, is this something new, has this been going on for 3, 4, 5 years? A decade?

Mr. LATHAM. I don't know the time period, but it is our understanding——

Mr. CORREA. Mr. Cline, could you help me out here?

Mr. CLINE. Absolutely, Chair Correa. It has been going on for a good while, sir. It is——

Mr. CORREA. I ask this because—first of all, let me say, thank you for the good work you do keeping us safe, our buildings, our citizens, our Federal employees.

Your job is finding a needle in a haystack, yet failure is unacceptable. Oklahoma City bombing, 9/11, when you have failures, they are big. It is not you, it is us. What I am trying to do is figure out a road map here to help you do your job better.

Seventy percent, help me out here, give me a little bit of a road map, a little bit of confidence. Tell me that you prioritize some of the things you need to do, because 70 percent of your recommendations not going implemented is not something I am comfortable listening to today. Mr. Cline, please.

Mr. CLINE. Thank you, sir, and as the representative from GAO mentioned, we have corrected the cost estimates for the countermeasures. So that is an approach that we have corrected.

It is very difficult to get these countermeasures implemented, and like we have mentioned, it is typically a lack of resources from the agencies to be able to implement those countermeasures.

If it is a multi-tenant facility, then all the agencies in the facility, No. 1, have to agree to that countermeasure recommendation, and No. 2, they have to fund their share of that cost for the countermeasure recommendation.

My counterpart at ISC, they recently established a program to observe the compliance by agency of the countermeasure rec-

ommendations. I think it might be worthwhile to have Mr. Breor talk to you a little bit about that, sir, and how we are doing that.

Mr. CORREA. Mr. Breor, in the few moments I have, please.

Mr. BREOR. Yes, sir. So under the risk management process which initially came out in 2013, one of the key aspects of that is you have a standard now compliance to that standard.

So we are working with our interagency partners, because I am here representing the collective, all 66 departments and agencies that make up the ISC.

At the end of that tail, it is that specific department, agency, that facility, that owns that risk.

What we rolled out in 2019, a compliance system, so we are now receiving reports from departments and agencies with respect to their compliance to the risk management process standard, active shooter, and also prohibited items into Federal facilities.

I am happy to say that this year, and going along with GAO best practices, we actually finished a pilot of a verification program. So it is one thing then to collect on a compliance, it is another thing to verify that compliance.

So going forward we will be able to verify what departments and agencies submit into the compliance system.

Mr. CORREA. I got further questions, but we are out of time, so I would like to recognize the Ranking Member of the subcommittee, the gentleman from Michigan, Mr. Meijer, for his set of questions.

Mr. MEIJER. Thank you, Mr. Chairman.

Obviously it is a difficult position you find yourselves in because you are making recommendations. You are, as the GAO noted, you are trying to get those recommendations—or when making those recommendations, trying to present and do so in a way that is going to be most conducive to them ultimately being adopted, while at the same time, having FPS personnel standing in that breach in the interim.

I think that was drove home by the death of PSO Patrick Underwood on May 29, 2020, you know, during the George Floyd protests. An accelerationist group took advantage of that chaos and shot and killed PSO Underwood and wounded his partner.

So I don't necessarily want to dwell on that one tragic incident, but how does FPS balance the desire to have those recommendations being implemented with the fact that it is FPS personnel, you know, who are protecting, especially on the PSO side, who are protecting, and potentially made vulnerable if those recommendations are not ultimately implemented by the facility owner? Mr. Cline, that is probably most appropriate to you.

Mr. CLINE. Thank you, sir. It puts us in a difficult situation when the countermeasures are not implemented. We balance our staffing requirements. We work with our local and city, county, State, Federal partners to maintain awareness of threats to facilities, demonstrations that may occur at those facilities, and we balance our deployment efforts and staffing efforts to those facilities based on what we hear.

I am with you on Pat Underwood, hero. Went to his memorial service out in Oakland. Bad situation. We had 17 FPS officers at that Federal building at the time of that incident, total chaos. Very

violent demonstration was occurring at the time, and like you said, bad actors took advantage of that situation.

So for us, it is a balance on how we deploy ourselves. We know by facility where the highest risks are and where we need to put people. So, for instance, the FBI facilities around the country, the field offices and resident agencies are very secure.

You observed that in Cincinnati during the attack. There is no way anyone was going to get inside that building. Our protective security officers sounded the alarm, and the FBI agents inside the building responded, and the individual fled.

Working to get the other agencies to reach that level of awareness and preparedness is our issue, but like it was mentioned before, it primarily comes down to the funding.

This is a multi-tenant agency in Ames, Iowa. They are working with their departments and agencies here in Washington, DC to get—and it could be—$20,000 was their portion of a camera—permanent camera project, and getting that $20,000 back to Ames, Iowa, is the difficult situation that the facility security committees find themselves in.

Mr. MEIJER. I want to follow up on one you said, Mr. Cline, but I don't want you to have to answer it.

Ms. Latham, Mr. Cline mentioned the FBI as a tenant organization that is both aware of the threat that they face and the critical role, and also very well-equipped to understand and to balance that threat versus the costs of the countermeasures.

Are there any—and this is why I didn't want Mr. Cline to have to answer it—are there any agencies, tenant agencies that you think are particularly less inclined to adopt countermeasures on the opposite end of the spectrum? If FBI is maybe in the better practices, who is in the worst?

Ms. LATHAM. Well, I would say, in terms of your question, not necessarily less inclined, but the agencies, when we did our review that we noticed had more recommendations that were not addressed were your more smaller agencies, which that could be understandable, from some of the comments that Chief Cline mentioned, maybe due to some of their challenges to address them. But we didn't look further into that. But I would say the smaller agencies compared to the larger ones had more unaddressed recommendations.

Mr. MEIJER. Thank you.

Mr. Cline, just wanted to get back to you real quick, a broader question. FPS has been transferred, as we mentioned, to three different parts of DHS in the last two decades. Do you think right now, the management directorate will be a permanent home for FPS, or is another home within DHS potentially more appropriate?

Mr. CLINE. Thank you, Ranking Member Meijer. Our transition to management has been wonderful. We are really taking advantage of the expertise of the lines of business. CFO, CRFO, you name it, I mean, we need to mature our business programs within FPS, and being under management is really helping us do that.

Ultimately the decision on the placement of FPS, I think as we grow and mature, we would be ready to prepare ourselves to become a component within DHS, a stand-alone component, but right now, our alignment with management, specifically under the lead-

ership and guidance of Acting Under Secretary for Management Mr. Alles, has been a good place for us right now.

Mr. MEIJER. Thank you, Mr. Cline, and with that my time is expired, and I yield back, Mr. Correa.

Mr. CORREA. Thank you, sir. The Chair will now recognize other Members of the committee for questions that they may wish to ask the witnesses.

In accordance with the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy, I will recognize Members in order of seniority, alternating between Majority and Minority Members, and Members are also reminded to unmute themselves when recognized for questions.

Now I would like to recognize Mr. Payne of New Jersey for 5 minutes of questions. Mr. Payne, welcome.

Mr. PAYNE. Thank you, Mr. Chairman, and thank you for having this timely hearing. Let's see.

Deputy—Mr. Cline, according to the Government Accountability Office, the Federal Protective Service is facing a staffing shortage with approximately 21 percent of its positions unfilled, including about 200 law enforcement positions.

How are you ensuring that FPS is still able to respond to threats to the Federal property, perform security assessments, and execute its other core missions while working with a reduced number of law enforcement personnel?

Mr. CLINE. Thank you for your question, Congressman Payne. You are correct, we are experiencing about a 21 percent shortfall on our staffing needs. It is a variety of reasons for this.

You know, like most other businesses and agencies within the United States, we are all dealing with labor market challenges, the same as everyone else. We are also competing for the same people. So city, county, State, and Federal law enforcement agencies are all looking for that same person to join their agencies and become a law enforcement officer.

We continue to work with DHS, Office of the Chief Human Capital Officer. Our recruiting team will be at a military base tomorrow to continue our recruiting efforts.

We just started a class at the Federal Law Enforcement Training Center last Monday, of 24 new students, and we have other classes scheduled for this year. So it is a continued challenge for us, but our goal in fiscal year 2023 is to fill all of our vacancies, including our law enforcement and our support position vacancies.

Mr. PAYNE. OK. Given what we have seen in the aftermath of January 6th investigations that uncovered both military and law enforcement personnel being involved in the insurrection, what is FPS doing to weed out the potential nature of these ideological folks amongst your ranks?

Mr. CLINE. Thank you for your question, Congressman. So when we recruit and hire a new officer, they go through the security clearance process through the DHS Office of the Chief Security Officer. Very rigorous process, very detailed and thorough analysis of the background and suitability of that applicant.

Once they come on board, the Office of the Chief Security Officer and DHS has also stood up a program, I don't know the exact name of it, sir, but it is basically continuous monitoring.

So if that individual that is—take me, for instance, if tonight I was arrested for some reason, that continuous monitoring program would—the Office of the Chief Security Officer would know about that tomorrow, and then they would take action on it, based on whatever that circumstance of the arrest was.

So it is our goal to make sure that the people we hire are not involved in any DBE-type activity. We do hire a large number of veterans. We have 80 percent of our law enforcement officers are veterans today. I am a veteran just like they are.

But the process that the Office of the Chief Security Officer uses to do that background investigation on the prospective employee and their continuous monitoring of the employee's activities is really helping us to make sure we weed out those bad actors.

Mr. PAYNE. OK. I think that was a focus on new hires. What about officers that are already in the organization?

Mr. CLINE. Yes, sir. That is the process that the Office of the Chief Security Officer uses on their continuous monitoring program. Also with our relationships with city, county, State, and Federal law enforcement, as you are aware, the law enforcement agencies actively monitor different types of media, looking for individual that may be associated with domestic violence extremism. If we receive notification or are aware of a DHS or an FPS officer, then that will be turned over to our Office of Internal Affairs to investigate that employee's activity.

Mr. PAYNE. Well, thank you.

Mr. Chairman, we have to stay vigilant in this area, because as we know, we have done an incredible job stopping the foreign fighter, but it is the internal issues that we have with domestic terrorism that plagues our Nation today. With that, I yield back.

Mr. CORREA. Thank you, Mr. Payne.

Now I recognize the gentleman from North Carolina, Mr. Bishop, for 5 minutes. Welcome, sir.

Mr. BISHOP. Thank you, Mr. Chairman.

Mr. Cline, I want to focus us on something that has almost slipped from National consciousness, but it always struck me as something very strange. In Portland, Oregon, over, I think June and July 2020, there were 52 consecutive nights in which antifa, anarchists, and other radicals, I guess, carried out violence. A lot of it focused on the Federal courthouse in Portland.

But one thing just sticks in my memory about that, is, I know that there were some reports at the time that officers, Federal officers were blinded or injured by lasers. How wide-spread was that? Have those officers recovered fully, or have there been permanent injuries resulting from that?

Mr. CLINE. Thank you, Congressman Bishop. Portland was a very chaotic, unprecedented event that we haven't seen before. A number of officers within FPS, 363 officers were injured. I think roughly a total of 800 injuries to not only the FPS officers, but also the CBP and ICE officers that provided us assistance, primarily with the green lasers, Molotov cocktails, ball bearings shot with sling shots, commercial-grade pyrotechnics that were thrown at them.

The FPS and DHS officers that supported that event are, in my eyes, they are heroes. I mean, they—their level of restraint, their

goal was to ensure that the courthouse and the Federal facilities in Portland were protected, and they achieved that goal. They stayed inside that courthouse until someone was attempting to cause damage, like setting the building on fire before they would come out, to take action, and then when they did come out, they were hit with a barrage of violence basically.

So all those officers have recovered from those injuries. We did have one—an FPS officer who did die of a heart attack not during the events, but as he was going to work. Then unfortunately, another officer within DHS did commit suicide, but we don't know if it was related to his activities in Portland, but he had served in Portland.

Mr. BISHOP. What an excellent summary of that, Mr. Cline. You started with the term "unprecedented," and that was how it struck, I think, many Americans, never seen anything like this in the terms of the continued activity over a long period of time.

One thing that was remarkable is that the Portland City Council voted, as I understand it, to prevent police from cooperating with Federal law enforcement. The mayor out there, Ted Wheeler, said at one point the presence of DHS officers is "actually leading to more violence and more vandalism."

He had mayors from a number of cities write the attorney general and the Acting DHS Secretary, saying that the deployment of officers to protect the facilities was an abuse of power.

I know that, if I understand GAO's report on DHS's strategy in Portland, suggested that there was an assumption you would receive support from local law enforcement, but that wasn't the case. So GAO recommended implementing a new strategy to account for that.

I hardly believe that I am reading words like that in a Congressional hearing or—and certainly that they would be true. What can you offer us about that issue? How do you intend to respond to the fact that mayors have supported and city council has supported that kind of lawlessness and refused to help?

Mr. CLINE. Thank you, Congressman Bishop. So throughout the country, we rely heavily on city, county, State law enforcement to assist us in the protection of our facilities.

Typically in a large city, if there is some type of violence or criminal act at a Federal building, the local law enforcement may be the first to respond.

The majority of Federal facilities that we protect are concurrent jurisdiction, meaning that the local law enforcement agencies have the ability to respond as well.

Within Portland, we—the fact that the Portland Police Bureau, who we are very tight with, we work well together with, the fact that they were prohibited from assisting us is the exact reason why we had to deploy more officers out there to protect the Federal facilities.

Typically, day to day, they will provide our assistance, but during that time frame, they were restricted and were not able to support us which caused us to deploy more people out there.

Mr. BISHOP. It seems to some of us that this kind of attack is something that can spring up in lots of places in the United States, that somebody is out there organizing it. Does that not need to be

looked into by Congress to determine whether people have the ability to bring this kind of attack against Federal facilities at any time they choose?

Mr. CLINE. Congressman Bishop, I think between the summer of 2020, which a lot of law—not just FPS, but a lot of law enforcement officers and agencies were dealing with large-scale demonstrations, and in some cases, some violence. You all experienced that on January 6, we experienced it out in Portland.

So, I think it is—we have done well working with our partner agencies in the Federal Government and city, county, State, shared information. We have all learned our lessons that we all need to work better together, sharing information, make sure we are aware of incidents that could pop up, and that has really increased over the last year.

Mr. BISHOP. Thanks for your outstanding service and testimony, and, Mr. Chairman, my time is expired.

Mr. CORREA. Thank you very much.

Now I call on the gentlelady from Nevada, Ms. Titus, for 5 minutes of questions. Welcome, ma'am.

Ms. TITUS. Well, thank you very much, Mr. Chairman. The previous Member of this committee was talking about Portland being an unprecedented event. Well, let's talk about another unprecedented event, and that was the storming of the Capitol on January the 6th.

Now, nobody could have anticipated it would be as terrible as it was, but there were certainly warning signs, including radical commentary on the internet for several days leading up to the events of that day, where people tried to—well, didn't try, they did—storm the Capitol and tried to overturn our legal elections.

It was hyperpartisan, it was neofascist, it was pro-violent, and it was racist. Should have given us some hint, because this was festering on-line for several days.

Now, we are not seeing that kind of incendiary language to that extent right now, but I think there are some lessons we can learn about how to spot potential events like this.

So I would ask Mr. Cline, how is your agency working with others to keep apprised of misinformation on-line and to stay aware of credible threats to Federal buildings that might come as a result of that, or in conjunction with that?

Does the interagency security committee factor in on-line threat environment when you are conducting your risk assessments of Federal buildings, and if you don't, why not?

Mr. CLINE. Thank you, Congresswoman Titus. As we mentioned before, we have dramatically increased our communication with our city, county, State, and Federal law enforcement partners.

We maintain regular and active communications with our law enforcement partners, DHS, intelligence, and analysis, the fusion centers throughout the country, the Federal executive boards, which are the 28 Federal executive boards throughout the country that have a level of oversight over the Federal agencies in their area of operation.

We continue to maintain awareness of threats. As you mentioned, sharing of information is critical to make sure that we are

all prepared to actively respond, react to a situation that may be coming up.

You mentioned January 6. On that day, our job, the Federal Protective Service, was to protect the Federal buildings that were in the area of the Ellipse and then the march that took place to the Capitol. That is what we were focused on.

We did provide—the U.S. Capitol Police requested support, and we did provide support to the Capitol as soon as that call went out.

But definitely, ma'am, the sharing of information, the preparation for events like this that could occur, has dramatically increased since January 6, and I think it is in a really good place now.

Ms. TITUS. Well, we certainly appreciate your help on that day in trying to keep all of the building, members, staff, press, everybody safe. So thank you for that.

Could you talk specifically about the Protective Investigations Program and how your members work there or train there, cooperate with them?

Mr. CLINE. Absolutely, ma'am. So, so far this year, we have opened up 201 protective threat investigations, and we have made 19 arrests at this point. We anticipate we will make more arrests as those investigations continue. Most of these threat investigations, we are informed from an agency of an employee who received a threatening communication, whether it is an email, phone call, text message, whatever it may be.

That information is provided to us, and our special agents, our criminal investigators will conduct the investigation, work with city, county, and State partners, Federal partners, to do the background on the bad actor, the person making the threat, and will make a determination coordinating with the Assistant U.S. Attorney, their office within that area that the threat is coming from, to make the determine on making the arrest. That is typically how that process works, ma'am.

Ms. TITUS. Well, thank you so much. You know, this committee really appreciates the job that you do, and understand how it might be hard to get people to work, to recruit, and also to maintain that force. So be sure you let us know what resources you need, if we need to provide additional funding or assistance in any way so you can do your job effectively.

Thank you, Mr. Chairman, I will yield back.

Mr. CORREA. Thank you, Ms. Titus.

Now I would like to recognize the gentlelady from Tennessee, Mrs. Harshbarger, for 5 minutes of questioning.

Mrs. HARSHBARGER. Thank you, Mr. Chairman, and Ranking Member, and thank you to the witnesses today, and honestly, I want to thank law enforcement for the job they do. You don't get enough thank yous these days.

The first question is for Mr. Breor. We have heard about FPS's process for assisting facility security, but there is many Federal facilities that are not under the FPS purview. My question is, what is ISC doing to ensure all these agencies have a robust security assessment process that complies with ISC standards?

Mr. BREOR. Thank you for the question. So this is back to 2019 where we released the compliance system. So the 66 departments

and agencies that make up the Interagency Security Committee, part of their compliance reporting, and everything that was framed around compliance was created by them through our compliance subcommittee.

So they are part of the process. Now they must report on what they are doing, both at the organizational level, headquarters, and at the facility level with respect to meeting the standards of the Interagency Security Committee.

I am happy to say that at least this year, we were able to run through a verification pilot. So going forward now, we will be able to work with the departments and agencies to actually verify what they are submitting into the compliance system so we can better monitor and track their submissions.

Mrs. HARSHBARGER. Yes, it is all about tracking what they need and measuring those outcomes.

I have a question for Ms. Latham. Facility security has been on GAO's high-risk since 2003, and what are the issues that are keeping these facilities' security on that high-risk list, and what are the actions that FPS can take to address GAO's concerns?

Ms. LATHAM. Thank you for your question. Yes, they have been on our high-risk list since 2003. There are two remaining items that need to be addressed.

FPS currently has two systems in place that they are working on and have been developing over time, and these systems first focus on what their learning activities are for officers, as well as to what extent the officers have completed training, as well as time and attendance.

We are looking for FPS to, No. 1, fully implement both of these systems, and in addition, make sure these systems are sort-of interoperable and sort-of coordinating together so they can know who meets the requirements, and more importantly, who should stand post and be ready.

Mrs. HARSHBARGER. Absolutely. FPS is a fee-for-service organization. Do you believe that is the best way for them to operate, ma'am?

Ms. LATHAM. I am sorry. The first part of your question, do you mind repeating?

Mrs. HARSHBARGER. FPS is a fee-for-service organization, and with that, do you believe that is the best way for them to operate?

Ms. LATHAM. Thank you. Well, we have certainly looked in sort-of components of the fee structure for FPS and just to see if there are any advantages or disadvantages to the structure that stands. We haven't done necessarily a whole review, but we certainly have, you know, made positive comments regarding that.

Mrs. HARSHBARGER. OK. Those are my questions, Mr. Chairman, and with that, I will yield back.

Mr. CORREA. Thank you, Mrs. Harshbarger, and now I recognize the gentleman from New York, Mr. Torres, for 5 minutes of questions. Welcome, sir.

Mr. TORRES. Thank you, Mr. Chair. I want to make sure I understand the process. So the Interagency Security Committee sets the physical security standards; the Federal Protective Service, FPS, makes security assessments and recommendations based on those standards; and a Federal buildings facilities security committee

must decide whether to comply with those recommendations. Is that how the process works?

Mr. CLINE. That is correct, Chair—or Congressman.

Mr. TORRES. OK. Now, if I scored 30 percent on an exam, I would receive an F, a failing grade. Am I right to see a compliance rate of 30 percent as a failure? Mr. Cline.

Mr. CLINE. Sir, the 30 percent is typically a failure. Variety of factors involved in making those decisions and the funding of those.

Mr. TORRES. I am just—so if it is a failure, like rather than tinker at the margins, should we not fundamentally rethink the model of voluntary compliance? Should security assessments be binding?

Mr. CLINE. So the new compliance implementation that the Interagency Security Committee is doing, that is—I don't want to call it a stick, but that is making the agencies that oversee an office in Ames, Iowa, it is making the agencies more aware of what those countermeasure recommendations are, and making them comply with an Executive Order, basically.

This is an Executive Order that came out in 1995, requiring these certain countermeasures to get the facility to the necessary level of protection.

Mr. TORRES. But there is no obligation to implement them, right? So it is ultimately a model of voluntary compliance. My question to you, is there any circumstance under which security assessments should be binding? What about the Level 5 Federal buildings where the security risk is highest, should it be binding under those circumstances?

Mr. CLINE. I think it definitely needs to have more influence, and I think requiring——

Mr. TORRES. Not influence, binding effect.

Mr. CLINE. Yes, requiring that it be implemented instead of requesting that it be implemented——

Mr. TORRES. Because if we do the same thing over and over again and expect a different result, that is the definition of insanity, as Albert Einstein said.

You said earlier, if I understood correctly, that in order for countermeasures to be implemented, you need all the tenants to agree. So it is not simply enough to have a majority, you need unanimity, and there could be scores of tenants in a single building. Like, that just strikes me as a process that breeds inertia and failure. How could we possibly defend that?

Mr. CLINE. So that is the Facility Security Committee that we talked about earlier, agreeing, because they all have to fund their portion of that countermeasure. Like I mentioned, if it is a $10,000 perimeter camera project——

Mr. TORRES. But one could imagine a model in which a majority of the committee agree, and then everyone is required to pay their fair share. That is a much more rational system——

Mr. CLINE. Correct.

Mr. TORRES [continuing]. Than expecting unanimity in every case. That is unrealistic.

Mr. BREOR. The weight of the vote on that committee is based on square footage of the tenant, so that there is a way to weight those that have more of a presence, they have a stronger vote.

Mr. TORRES. So would you be in favor of substituting a majority requirement for a unanimity requirement?

Mr. BREOR. That is something that we can look at.

Mr. TORRES. OK. It just seems to me that that would facilitate compliance. What about staffing 1,000 law enforcement security officers who are responsible for a portfolio of 9,500 buildings? It would seem to me that the scale of your responsibilities are just proportionate to the scarcity of your resources. Do you have the staff you need to sufficiently secure 9,500 buildings? Is a thousand enough?

Mr. CLINE. Sir, so our current goal is to fill our current vacancies; get those done. As we have, if the threat environment continues to escalate as it has, and you know we have got——

Mr. TORRES. Well, let's assume there is no escalation. You have 9,500 buildings you have to protect. Let's assume you fill all your vacancies. It just seems to me 1,000 is a small number, given the size of your portfolio.

Mr. CLINE. Sir, our authorized strength for law enforcement is 1,131. They are placed throughout the country based on the number of facilities, population of the Federal employees there, threats. You know, their highest-risk facilities would have more people. We have more officers here in the District of Columbia than we have in Ames, Iowa, primarily, because they are needed here.

Mr. TORRES. But like the Capitol Police has thousands of officers for one complex. You have 1,000 officers for 9,500 buildings. There seems to be a disconnect there. But my time has expired.

Mr. CORREA. Thank you, Mr. Torres. I wanted to—sir, I want to go through a second round of questions, and I wanted to follow up on Mr. Torres' concept here. You have got tenants. They are supposed to pay you their fair share.

Ms. Latham, you said one of the big issues is money to implement. Like Mr. Torres says, 30 percent compliance, 70 percent none. Do we have to mandate that other Federal agencies pay their fair share of what you recommend, what you prioritize that needs to be done to secure these buildings?

Mr. CLINE. Thank you, Mr. Chairman. There is no mandate. There is no law that requires it.

Mr. CORREA. We need one. If the FBI—if other Government agencies have X number of dollars—and you have just said you need to invest the following to protect the building, your personnel, and citizens to actually come to visit your buildings. This has been going on for a number of years noncompliance. This is unacceptable. What do we need to do to mandate that the financing be there, be reallocated, so to speak, to make sure that at least the set of priorities to secure these buildings is actually addressed?

Mr. CLINE. Sir, it is a critical issue for us. With Scott being or Mr.—my counterpart from the ISC being here and working directly with those departments and agencies——

Mr. CORREA. Mr. Breor.

Mr. BREOR. Yes, sir. We are seeing, since monitor and compliance since 2019, we are seeing an improvement each year. A couple of issues that do arise, and what we are working on now is the internal guidance within the departments and agencies on how to im-

plement the ISC standards within their organization, and then follow on to that guidance and policy from the headquarters——

Mr. CORREA. I hear your words, but I am still concerned. You haven't alleviated my concerns because as, you know, all of you are out there doing a good job protecting us citizens, but yet now essentially the threats are turning on you, on us. I am trying to assess, in my mind, factually, here from your statements whether you are prepared to play defense as well. I am not getting a good vibe out of your statements today. Thoughts?

Mr. BREOR. I think where we are with respect to the Federal security committees that run the multi-tenant facilities, we have rolled out training, we are rolling out workshops. We now have regional advisors that are across the United States that are helping these FSCs. So I think the facilities that have tenants, I think there is work that needs to be done so that they better understand the ISC.

Mr. CORREA. I am hearing your words. I would like to get more of an assurance that we are going to move to better compliance here and the priorities or things that need to be done to harden these buildings to make sure that they are not vulnerable to these senseless attacks, you know, actually take place.

None of us here, none of us here condone attacks on our Federal officers, Federal personnel, as well as our U.S. citizens.

Let me shift real quick. Mr. Cline. Mr. Bishop talked about Oregon. He talked about coordination. That was an ugly situation. Unprecedented, your words. Something that none of us condone. I don't like seeing—or I disagree. I would do everything I can to stop our Federal officers from being attacked. If you talk about coordination, you extended your authority to CBP and ICE to help in that situation, and yet, the local Portland law enforcement officials didn't want to see that happen because of the controversy, the local elements there that essentially, my words, maybe inflamed the situation. How can we move forward to make sure there is better coordination here? You're at the Feds, they're at the local, you got to figure out this situation, a situation before it gets out of control. Mr. Cline, lessons learned.

Mr. CLINE. Thank you, Chairman. We have learned a number of lessons out of Portland. We rely heavily on city, county, State law enforcement to support our mission. As Mr. Torres mentioned, we are a small agency. You know, for us to—we don't want to create a Federal police force across the Nation. We rely heavily on our contracted protective security officers to protect our facilities.

Right now, there is about 6,200 PSO posts that are staffed this minute; X-ray machine, magnetometer, roaming patrols, monitoring cameras, perimeter security that we rely heavily on.

We made a lot of changes after Portland. Our public order policing doctrine, we signed that in June 2021. A new directive on how we approach public order. The use of force policy and directive is in—with the director for signature right now. That was coordinated with civil rights and civil liberties, the Office of Privacy, the Office of Policy, and we have managed to change the process on how we approach civil disorder.

As far as utilizing CBP and ICE, that was necessary because the local law enforcement, Portland Police Bureau who we work hand-

in-hand with day-to-day, during that instance they were prohibited from assisting us. The Multnomah County Sheriff's Office, the Portland Oregon State Police, they came in at times to assist, but the locals were prohibited. We don't see that anywhere else. We think it is done in Portland that we no longer have that situation.

Mr. CORREA. Thank you very much. I ran out of time, so I am going to have Mr. Meijer—your line of questions, sir.

Mr. MEIJER. Thank you, Mr. Chairman. I want to follow up a little bit on what Mr. Torres was asking about and just to clarify, the FSCs.

Now, obviously, any assessment or responsibility for the security upgrades or countermeasure implementation are shared on like a pro rata basis within the tenants. But for the FSC, it does have to be unanimous support of all members of that to adopt a recommendation. Is that correct?

Mr. BREOR. The FSC, the tenant members are given a way with respect to their vote based on square footage.

Mr. MEIJER. Uh-huh.

Mr. BREOR. So if you had a facility with three members, and one of those members' square footage was 66 percent, then their vote would be the driving force. The other two members out of majority could not, you know, go against the decision to move forward.

Mr. MEIJER. OK. So just to build on his line of questioning, it is a majority of the FSC?

Mr. BREOR. Based on square footage.

Mr. MEIJER. Based on square footage. OK. Thank you, because I think there has been some misunderstanding about unanimity versus majority opinion.

Getting back to the reasons why they are not implemented. I mean, in the GAO report, there is some very explicable reasons, right? An agency is planning to move, and so, if you are only going to be in a facility and the lease is running out in 2 years, it doesn't make sense. Maybe make sufficient upgrades. I think the other one was, you know, obviously the implementation costs is—so you are going to have a range.

Are there—but I guess kind-of building on that prior question, in some of those situations, it may be a facility that is a smaller facility and an individual stand-alone lease facility. I think oftentimes in our mind we have a conception of the main massive Federal building when you may have a Social Security agency outpost, and it is just renting a few, or a couple hundred or a couple thousand square feet in one facility, right? So we are talking about a blend.

But I guess my question is, are there—to what extent on—and I recognize this is more of a GSA question—but to what extent, or there may be recommendations to, if a smaller agency, a smaller footprint says these are not affordable or cost-effective upgrades for us given our logistical circumstances, are there ways where—you know, but they chose that location because it was relatively less expensive than maybe a higher, more secured facility was leasing on a per-square foot basis.

I think, Mr. Cline, you are not—I think you kind-of understand where I am getting at here. Obviously, FPS's is in more of an advisory role when offering these countermeasure recommendations, the cost-benefit analysis of each individual recommendation is

going to be dependent on that agency. But they are also making a cost-benefit analysis in a sort-of separate tranche on their individual leasing side.

Does FPS offer recommendations prior to GSA approving or suggesting a lease location for the agency?

Mr. CLINE. Thank you, Ranking Member. Yes, absolutely. So let's say an agency decides they want to move to a new location in Dallas, GSA will make contact with us, and we will go with GSA and the agency, and we will do pre-lease assessments.

So this is to go out and look if GSA has a port—here is some offerings from the lessees in the city. You have got these many people, this much square footage. You need this kind of space, and then we will go out and look at it. Then we will kind-of narrow that down to the top three, and then GSA will work with the agency to establish the lease. Then we will work with the agency to establish the necessary level of protection for that facility.

We want to get in there first before they move in. Let's get this established now before people are here. Let's get the projects in place. On a number of instances, if the agency says, I can't afford to do 20 cameras around my building. Then, well, if you can't do that, can we do at least cameras at every entrance, so we can see who is coming into the building, record some type of nefarious activity that goes on there? Let's come up with something. Let's don't leave it like we can't afford to do anything. Let's try to do something that takes sense, that helps us secure the facility.

Mr. MEIJER. But to be clear, prior to that lease being signed they understand, OK, maybe this facility that is in compliance already with what FPS might recommend, you know, that is $30 a square foot, this facility that is $25 a square foot, if it is, you know, if we are going only on a cost basis, I don't want that agency taking the lower-cost one. They may have to add another $10 per square foot in security improvements, right? So you are doing that prior to those leases being finalized.

Mr. CLINE. Yes, sir, absolutely. Mylar or window protection on the first floor of the building. A number of facilities that are offering to be leased to the Government have that already. So, if that has it there, that is one less countermeasure we have to implement because it is already in place.

Mr. MEIJER. Thank you. I yield back, Mr. Chairman.

Mr. CORREA. Thank you very much. Any other Members wish to ask questions of our witnesses? Seeing no further questions, I want to thank our witnesses today for your testimony and Members for their questions. Members of the committee may have additional questions for the witnesses, and we ask that you respond to those written questions expeditiously. The Chair reminds Members that the committee record will remain open for 10 days. Without objection, this committee stands adjourned. Thank you.

[Whereupon, at 11:25 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN J. LUIS CORREA FOR RICHARD "KRIS" CLINE

Question 1. According to the Government Accountability Office, the Federal Protective Service (FPS) is currently facing a staffing shortage, with approximately 21 percent of positions vacant, including about 200 law enforcement officer positions.

What steps is FPS taking to fill these vacant positions and when does it expect to fill the positions?

Answer. The Federal Protective Service (FPS) projects on-boarding approximately 100 Law Enforcement (LE) officers in fiscal year 2023, and another 150 LE officers over fiscal years 2024 and 2025. At the same time, FPS is working to reduce attrition and identify additional opportunities to recruit and on-board personnel. In calendar year 2022, FPS attended 45 job fairs at 50-plus locations and, to date, has extended over 275 tentative job offers to prospective employees who are currently in various stages of pre-employment processing. Our recruitment activities project that FPS will continue to recruit 30 to 50 prospective law enforcement officers per month.

Given the current environment and FPS's critical mission, it is paramount that we fill these vacancies. FPS is competing with other Federal, State, and local law enforcement agencies, as well as the private sector to attract the most qualified applicants. One area where FPS is disadvantaged is in its efforts to fill vacancies due to the discrepancy in law enforcement retirement coverage for its uniformed law enforcement officers, compared to other services. This needs to be addressed to allow FPS to recruit, hire, and retain a world-class workforce.

Question 2. Part of the Federal Protective Service's (FPS) core mission is to provide regular security assessments for Federally-owned and -leased property to identify and evaluate potential risks and make recommendations to improve protective measures. These security improvements can include things such as new security cameras, physical access control systems, and X-ray screening equipment. However, a recent review by the Government Accountability Office has found that all too often these needed improvements go unimplemented by the tenant agencies who lease, own, and operate Federal buildings.

What challenges does FPS face when tenant agencies do not implement security recommendations and does the failure to implement these recommendations require FPS to provide additional resources to ensure that Federal property is adequately secured?

Answer. Should the Facility Security Committee (FSC) decide to not accept, fund, or implement recommendations stemming from security assessments for Federally-owned and -leased property, FPS faces an increased challenge in meeting its mission. In these instances, the risk accepted through the risk management process is transferred to FPS and FPS must still work to secure Government facilities, protects Government employees and visitors, and ensures the safety, security, and continuity of Government services to the best of its ability.

FPS maintains a regular physical presence at many high-profile/high-risk locations throughout its protective inventory. However, based on the number of facilities compared with the number of law enforcement officers, FPS relies on technical countermeasures and contract Protective Security Officers (PSOs) to identify suspicious activities and serve as a warning system for criminal activity at most Federal facilities.

When countermeasures are not implemented, or vulnerabilities are not mitigated, FPS utilizes the latest intelligence information to prioritize its limited resources to mitigate vulnerabilities by, for example: Increasing visible patrols at selected facilities; increasing the number and locations of targeted explosive detection canine sweeps; conducting additional tenant security awareness briefings; increasing the number of internal and external patrols by its PSOs (if available on-site); seeking

additional support from local security and law enforcement partners; or some combination thereof.

QUESTIONS FROM CHAIRMAN J. LUIS CORREA FOR SCOTT BREOR

Question 1a. The Interagency Security Committee (ISC) is tasked with tracking and responding to an ever-evolving threat environment to ensure that Federal facilities have protective measures in place to deter the most relevant security threats and respond to new technological advancements.

What are the key emerging threats to Federal facilities and how is the ISC helping agencies prepare to address those threats?

Answer. The key emerging threats to Federal facilities are the continued rise in domestic violent extremism and nefarious cyber events. According to the June 2022 DHS National Terrorism Advisory System Bulletin, the United States remains in a heightened threat environment and several recent attacks have highlighted the dynamic and complex nature of the threat environment. It is expected that the threat environment will become more dynamic as several high-profile events could be exploited to justify acts of violence against a range of possible targets. These targets could, among others, include Government facilities and personnel.

To mitigate these threats and many others, the Interagency Security Committee (ISC) continues to develop and refine facility security standards and policies in response to emerging threats. This includes developing best practices and countermeasures in response to emerging threats. For example, the ISC's Best Practices Subcommittee published *Protecting Against Violent Civil Disturbance: Considerations for Federal Facilities* in response to increased domestic violent extremism threats. To counter the cyber threats, the ISC Risk Management Process standard details recommended 6 countermeasures specifically designed to mitigate unauthorized access, interruption of services and modification of services. The ISC also conducts outreach and facilitates information sharing to ensure organizations are aware of the latest threats and how to counter them. This is typically done through the development and publication of an annual threat report and focused and timely distribution of intelligence products. Last, the ISC provides training to build individual and organizational capacity to meet security standards. This is accomplished through independent study, instructor-led training and virtual instructor-led training to ensure Federal facility security stakeholders can access these capacity-building efforts whenever and wherever they might be located.

Question 1b. What emerging threats are agencies not currently focused on that they should be preparing to address?

Answer. Departments and agencies must be prepared for a range of threats from the traditional, such as active shooter and vehicle ramming; to emerging, such as cyber and unmanned aircraft systems. In preparing for this array of threats, organizations must prioritize risk given finite resources. At the Department and agency level, the ISC is encouraging organizational headquarters to maintain a centralized list or "risk register" to prioritize security efforts and support annual budget submissions. At the facility level, the ISC provides training on the Risk Management Process standard. In addition to these capacity-building efforts, the ISC validates organization risk assessment tools and training programs to ensure they meet ISC standards. Finally, the Cybersecurity and Infrastructure Security Agency's regional personnel work closely with the Federal Protective Service to bring the full capabilities of the U.S. Department of Homeland Security to bear to address emerging threats.