FACILITY PROTECTION: IMPLICATIONS OF THE NAVY YARD SHOOTING ON HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

OCTOBER 30, 2013

Serial No. 113–40

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

87–184 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
MARK SANFORD, South Carolina
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

JEFF DUNCAN, South Carolina, *Chairman*

PAUL C. BROUN, Georgia
LOU BARLETTA, Pennsylvania
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana, *Vice Chair*
MICHAEL T. MCCAUL, Texas *(Ex Officio)*
RON BARBER, Arizona
DONALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

RYAN CONSAUL, *Subcommittee Staff Director*
DEBORAH JORDAN, *Subcommittee Clerk*
TAMLA SCOTT, *Minority Subcommittee Staff Director*

CONTENTS

FACILITY PROTECTION: IMPLICATIONS OF THE NAVY YARD SHOOTING ON HOMELAND SECURITY

Wednesday, October 30, 2013

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

The subcommittee met, pursuant to call, at 9:32 a.m., in Room 210, Cannon House Office Building, Hon. Jeff Duncan [Chairman of the subcommittee] presiding.

Present: Representatives Duncan, Hudson, Barber, and O'Rourke.

Also present: Representative Jackson Lee.

Mr. DUNCAN. All right. The House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency will come to order.

The purpose of this hearing is to examine what the Department of Homeland Security is currently doing to protect Federal facilities and what steps, if any, need to be taken to improve current layers of security, so that incidents such as the Navy Yard shooting do not occur in the future.

Now, this isn't our normal committee room, so we are going to work through some things today, I am sure.

But I will now recognize myself for an opening statement.

The events that took place on September 16 at the Washington Navy Yard, less than 2 miles from where we are right now, were shocking and tragic. Twelve innocent lives were lost that day, along with several injured. Our thoughts and prayers go out to the families of the victims and those survivors and the folks that work as co-workers in the Navy Yard.

While much of the security of this horrific event will rightly focus on how someone in Aaron Alexis' mental state was able to pass a Governmental background investigation and to hold a security clearance, today's hearing will concentrate on the physical preventative security measures that are currently in place for our Federal facilities.

How do we control access to these facilities to protect both employees and public visitors? What physical security measures, if any, can be taken to prevent future tragedies?

The Federal Protective Service, or FPS, is charged with protection of Federal facilities and safeguarding Federal employees, contractors, and visitors within those facilities.

FPS is the primary agency for protecting and securing almost 50 percent of the General Service Administration's, or GSA's, owned or leased properties. That is about 9,600 facilities Nation-wide.

As the front-line personnel charged with the daily safety of Federal employees and visitors, it is crucial that this workforce is adequately trained and prepared to respond at moment's notice.

I strongly support the public/private partnership model that DHS uses with the contract guard force. Having private guards can increase the accountability for the taxpayer, but DHS cannot be deficient in its management responsibilities and must deploy the right number of guards, based on risk.

Unfortunately, according to the Government Accountability Office, or GAO, report that was released today, the Federal Protective Service has many weaknesses with the oversight and management of the guard program.

For example, FPS continues to lack effective management controls to ensure that all guards have met their certification and training requirements.

GAO has previously urged FPS to develop a management control system to document and verify training in reports submitted to Congress in 2010 and 2012, but FPS has yet to implement this recommendation.

Without such a system, how can FPS know and ensure that its guard force is sufficiently trained?

It seems common-sense to me that FPS should be able to verify that its guards are trained and certified properly, especially when others trust and rely on FPS guards for their protection.

One of the most shocking findings in the most recent GAO report is FPS' inadequate approach to active-shooter scenarios.

From the Holocaust Museum shooting in 2009 and the Navy Yard shooting to the most recent Federal courthouse shooting in Wheeling, West Virginia, in October, examples exist of the risk FPS and facility guards must confront from active-shooter scenarios. While FPS does require its guard force to receive training on active-shooter situations, it is unclear how this training is conducted and for what length of time.

GAO also noted that not all guards receive this training, and, even for those that have, it is unclear how their contract guards are expected to respond to an active shooter.

According to DHS, if an active shooter is not in a guard's line of sight, that guard's actions are then dictated by his or her post orders. So, does that mean that if an active shooter is in the building, killing innocent people, an armed guard is not allowed to assist until Federal or local law enforcement arrive at the scene?

If this is the case, then DHS' bureaucratic process is putting lives at risk.

The American people need to know how these guards can protect them in life-threatening situations, and I am looking forward to DHS providing clarity on this issue today.

As an additional layer of security, Federal employees are required to carry valid identification credentials for admittance into

Federal facilities. As a Federal Government contractor, Aaron Alexis had valid identification, which gave him access to the Naval Sea Systems Command headquarters, and that enabled him to pass through security.

While some buildings only require an ID to be used as a flash pass or visually inspected, other facilities require verification by use of a credential access control system, or swiping of the card.

Although the second scenario may provide higher security against individuals using fraudulent or expired and flagged credentials, it was discouraging to learn from my staff that DHS officials informed them that the department currently is not aware of the type of access control systems in place across DHS facilities.

How, after 10 years, does the Department not have a handle on what measures are in place to secure their own employees, let alone the general public, at Federal facilities?

I want to know precisely what DHS is doing to obtain this information and when it will have a full and complete grasp of the issue.

Considering the heinous events which took place just close by at the Navy Yard, it is important to ensure that the security framework in place at our Federal facilities is strong and effective.

The Federal Protective Service and its contract guard force put their lives on the line every day on a daily basis to protect the American people, and I want to thank them for their service and the tremendous amount of heroism that was exhibited in the Navy Yard.

I hope this hearing can serve as an opportunity to assess the state of physical security across Federal facilities and what DHS must do to improve the protection of employees and visitors to these facilities and prevent future tragedies as we recently witnessed.

[The statement of Chairman Duncan follows:]

STATEMENT OF CHAIRMAN JEFF DUNCAN

OCTOBER 30, 2013

The events that took place on September 16 at the Washington Navy Yard—less than 2 miles from where we are right now—were shocking and tragic. Twelve innocent lives were lost that day along with several injured.

While much of the scrutiny of this horrific event will rightly focus on how someone in Aaron Alexis's mental state was able to pass a Government background investigation and to hold a security clearance, today's hearing will concentrate on the physical preventative security measures that are currently in place at our Federal facilities. How do we control access to these facilities to protect employees and public visitors? What physical security measures, if any, can be taken to prevent future tragedies?

The Federal Protective Service (FPS) is charged with the protection of Federal facilities and the safeguarding of Federal employees, contractors, and visitors within those facilities. FPS is the primary agency for protecting and securing almost 50% of the General Services Administration's (GSA) owned or leased properties. That's about 9,600 facilities Nation-wide. As the front-line personnel charged with the daily safety of Federal employees and visitors, it is crucial that this workforce is adequately trained and prepared to respond at a moment's notice.

I strongly support the public-private partnership model DHS uses with the contract guard force. Having private guards can increase accountability for the taxpayer but DHS cannot be deficient in its management responsibilities and must deploy the right number of guards based on risk.

Unfortunately, according to a Government Accountability Office (GAO) report that was released today, the Federal Protective Service has many weaknesses with the

oversight and management of their guard program. For example, FPS continues to lack effective management controls to ensure that all guards have met their certification and training requirements.

GAO has previously urged FPS to develop a management control system to document and verify training in reports submitted to Congress in 2010 and 2012, but FPS has yet to implement this recommendation. Without such a system, how can FPS know and ensure that its guard force is sufficiently trained? It seems commonsense to me that FPS should be able to verify that its guards are trained and certified properly—especially when others trust and rely on FPS guards for their protection.

One of the most shocking findings in this most recent GAO report is FPS's inadequate approach to active-shooter scenarios. From the Holocaust Museum shooting in 2009, and the Navy Yard shooting to the most recent Federal courthouse shooting in Wheeling, West Virginia in October, examples exist of the risks FPS and facility guards must confront from active-shooter scenarios.

While FPS does require its guard force to receive training on active-shooter situations, it is unclear how this training is conducted and for what length of time. GAO also noted that not all guards received this training, and even for those who have, it is unclear how their contract guards are expected to respond to an active shooter.

According to DHS, if an active shooter is not in a guard's line of sight, that guard's actions are then dictated by his or her post orders. So does that mean that if an active shooter is in the building, killing innocent people, an armed guard is not allowed to assist until Federal or local law enforcement arrive at the scene? If this is the case, then DHS's bureaucratic process is putting lives at risk. The American people need to know how these guards can protect them in life-threatening situations. I am looking forward to DHS providing clarity on this issue today.

As an additional layer of security, Federal employees are required to carry valid identification credentials for admittance into Federal facilities. As a Federal Government contractor, Aaron Alexis had valid identification which gave him access to the Naval Sea Systems Command headquarters which enabled him to pass through security.

While some buildings only require an ID to be used as a "flash pass" or visually inspected, other facilities require additional verification by use of a credential access control system, or "swiping" of the card. Although the second scenario may provide higher security against individuals using fraudulent or expired and flagged credentials, it was discouraging to learn from my staff that DHS officials informed them that the Department currently is not aware of the type of access control systems in place across DHS facilities.

How, after 10 years, does the Department not have a handle on what measures are in place to secure their own employees, let alone the general public at Federal facilities? I want to know precisely what DHS is doing to obtain this information and when it will have a full grasp of this issue.

Considering the heinous events which took place at the Navy Yard, it is important to ensure that the security framework in place at our Federal facilities is strong and effective.

The Federal Protective Service and its contract guard force put their lives on the line on a daily basis to protect the American people, and I thank them for their service. I hope this hearing can serve as an opportunity to assess the state of physical security across Federal facilities and what DHS must do to improve protection of the employees and visitors to these facilities and prevent future tragedies.

Mr. DUNCAN. The Chairman will now recognize the Ranking Member of the subcommittee, the gentleman from Texas who is sitting in for the Ranking Member, Mr. Barber. But the gentleman from Texas, Mr. O'Rourke, is recognized for an opening statement.

Mr. O'ROURKE. Thank you.

I want to thank Chairman Duncan for calling and organizing today's hearing.

I want to thank the witnesses for their testimony, in advance, and I want to thank them in advance for answering our questions.

I want to thank the committee staff from both sides for doing all the leg work to get us ready for today.

I also want to extend my condolences to the families and survivors from those horrific events last month.

I know that any time there is a hearing like this or the issue reappears in the news, that has to open up those memories again, and must cause some additional pain and heartache for those who are involved.

So I want to make sure that we use today's hearing to learn what we can from what took place, and to apply those lessons to ensuring or trying to ensure that we don't have a repeat of this event at a Federal facility in the future.

I also want to make sure that we are proportionate in our response to what we learn. As the Chairman said, we want to have the right number of guards proportionate to the risk that we understand to take place.

These are, after all, public buildings. We want to make sure that we don't so fortify them that we exclude the public, that we create an impression that the public is not welcome, that we make it unduly difficult for people to access Government, to receive the services that they are paying for. They should have the right to expect to access.

I also hope that we will be able to explore the true cost of contracting services, using contractors versus dedicated civil servants or professionals who are in those jobs for their careers. There is a balance that we have to strike in terms of cost savings and efficiencies versus some level of dependability and building a culture that might, in fact, ultimately prevent these kinds of activities in the future.

I hope that, in closing, and I want to be brief because I want to get to the testimony from our witnesses, I hope that we use what we learn from horrific events like these—and unfortunately there are far too many over the last few years—to strike that right balance in all of those areas.

So I look forward to the testimony, to applying those lessons, to the Chairman's leadership in making sure that we strike that balance. With that, I will conclude and yield back to the Chairman.

Mr. DUNCAN. I thank the gentleman from Texas.

Other Members of the subcommittee are reminded that opening statements may be submitted for the record.

[The statements of Ranking Members Barber and Thompson follow:]

STATEMENT OF RANKING MEMBER RON BARBER

OCTOBER 30, 2013

Thank you, Chairman Duncan, for holding this very important hearing to examine how extensively standards for Federal facility security are being followed to ensure the safety of Federal personnel and visitors to these buildings.

Across the country, we are experiencing a rise in attempts by individuals to shoot at or otherwise attack Federal facilities, and it is both timely and critical that we hear today from Department officials and other witnesses about the efficacy of the standards put in place by the Interagency Security Committee to protect our people as well Federal facilities.

In addition to my own personal experience as the unintended victim of a shooting incident, we seem to get all-too-frequent news reports of attempts by mentally unstable or disgruntled individuals who open fire at Federal facilities.

I will be interested to hear today from the witnesses how effective they think the Interagency Security Committee has been to date not only in establishing a set of physical security standards, but also in providing enough guidance to Federal agencies and departments to increase their adoption of these standards.

It is not sufficient to issue standards—it is also incumbent upon the Interagency Security Committee and the Federal Protective Service, or FPS, as the implementing agency to make sure that Executive branch agencies understand how the Government's standards for physical security can best be utilized.

In the Government Accountability Office or GAO report issued at Ranking Member Thompson's request in January, GAO states that the Interagency Security Committee's standards are frequently the second choice of Federal physical security managers after their own institutional knowledge.

This is a troubling finding by GAO, and given the recent uptick in attempted shootings at Federal facilities, it is incumbent upon all of us to assist the Interagency Security Committee in strengthening its outreach and guidance regarding its standards for the safety of all Federal personnel and visitors.

In addition, GAO states in their testimony that Federal facility security is further jeopardized by FPS' on-going mismanagement of its contract guard force, and alarmingly, but the agency's failure to ensure that its guards receive the required active-shooter response training that would best prepare them to protect Federal facilities.

Further, GAO's testimony indicates that FPS and several other Federal agencies are not currently using an appropriate methodology to assess risk at Federal facilities which only increases the vulnerability of those who work in or visit Federal buildings. I look forward to hear the witnesses address these and other pertinent issues related to Federal facility security.

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

The purpose of this hearing is to review the security protocols in place to safeguard Federal facilities and the Federal personnel who work within them, and the visitors to those buildings. I am a long-standing observer of the Federal Protective Service, or FPS, and at the beginning of this Congress, I reintroduced my legislation, H.R. 735, the Federal Protective Service Improvement and Accountability Act of 2013. My legislation seeks to move FPS away from its over-reliance on contract security guards, and to instead build up the agency's internal capacity.

Also, at my request, the Government Accountability Office has produced 10 reports related to FPS, the most recent of which pertains to today's topic of Federal facility security protocols and which was released in January of this year. We are all cognizant of the recent shooting at the Navy Yard on September 16, yet incidents of active shooters who breach Federal facilities have become all too commonplace.

In my own home district of Jackson, Mississippi, a man was arrested on October 2 for attempting to walk inside the Veterans Affairs regional affairs office with a pistol and was then recommended to undergo a psychiatric evaluation. Some other recent examples of individuals who have attempted to open fire on Federal facilities include a former police officer in Wheeling, West Virginia who fired more than 20 shots at a Federal courthouse located there on October 8 of this year; on February 15, 2012, an ICE agent shot and killed one colleague and wounded another in the Federal building in Long Beach, California; and a bag containing an improvised explosive device, or IED, was left undetected for several weeks inside the Federal building in Detroit, Michigan in February 2011. An FPS contract guard brought the bag inside the building and placed it under a screening console where the IED remained in the bag until it was discovered 21 days later.

Clearly, we must ensure that the personnel who oversee physical security programs at our Federal facilities are adhering closely to the uniform set of standards provided by the Interagency Security Committee. In 1995, after the bombing of the Alfred P. Murrah Federal building in Oklahoma City, President Bill Clinton signed Executive Order 12977. As an outcome of Executive Order 12977, the Interagency Security Committee was created to produce a coherent set of physical security standards that can be tailored to meet the diverse needs of Federal agencies and departments.

This hearing should allow us to determine how closely Federal agencies and departments are complying with the Interagency Committee's security protocols, and demonstrate what remaining outreach work DHS must undertake to make sure that its physical security protocols are being implemented and adhered to in the interest of National safety.

Mr. DUNCAN. We are pleased to have a distinguished panel of witnesses before us today on this important topic. Let me remind the witnesses that their entire written statement will appear in the record.

I will introduce each of you first and then I will recognize you individually for your testimony.

Members of the Committee may come and go today. There is a lot going on on the Hill with mark-ups and other committee hearings on a Wednesday morning. So Members may come and go as the committee progresses.

So let me start off by introducing the witnesses. The first one is Mr. L. Eric Patterson. Eric was appointed director of the Federal Protective Service, a subcomponent of the National Protection and Programs Directorate of the Department of Homeland Security in September 2010.

Mr. Patterson previously served as deputy director of defense, counterintelligence, and HUMINT center at the Defense Intelligence Agency, DIA. Prior to joining DIA, Mr. Patterson served as a principal with Booz Allen Hamilton, where he supported two of the Defense Technical Information Center analysis centers.

Mr. Patterson is a retired United States Air Force brigadier general with 30 years of service.

Sir, thank you for your service to our great Nation.

Mr. Greg Marshall is the chief security officer for the Department of Homeland Security. In this capacity, Mr. Marshall is responsible for security-related issues effecting the Department personnel security, physical security, special security, special access programs, security training and awareness.

Mr. Marshall began his Federal career as a police officer with the United States Capitol Police in 1984 and later transferred to the Howard County Maryland Police Department where he retired in 2007.

He returned to Federal service when he joined DHS as deputy chief of physical security and was later promoted deputy chief security officer.

Ms. Caitlin Durkovich is the assistant secretary for infrastructure protection at the Department for Homeland Security. In this role, she leads the Department's efforts to strengthen public-private partnerships and coordinate programs to protect the Nation's critical infrastructure, assess and mitigate risk, build resilience, and strengthen instant response and recovery.

Previously, Ms. Durkovich served as the National Protection and Program Directorate as chief of staff, overseeing day-to-day management of the director and the development of internal policies and strategic planning.

She is testifying on behalf of the inter-agency security committee, a committee comprised of 53 representatives of Federal agencies and departments with the mandate to enhance the quality and effectiveness of physical security of Federal buildings in the United States.

Last, Mr. Mark Goldstein is the director of physical infrastructure issues at the GAO. Mr. Goldstein is responsible for GAO's work in the areas of Government property, critical infrastructure, and telecommunications.

Mr. Goldstein has held other public-sector positions including serving as the deputy executive director and chief of staff to the District of Columbia financial control board, legislative adviser of the commissioner of internal revenue, and a senior staff member

of the United States Senate Committee on Homeland Security and Governmental Affairs.

Prior to Government service, Mr. Goldstein was an investigative journalist and author.

We can see that we have got a great panel here today and I look forward to your testimony. So I want to thank you all for being here. I now recognize Mr. Patterson for his opening statement.

STATEMENT OF L. ERIC PATTERSON, DIRECTOR, FEDERAL PROTECTIVE SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PATTERSON. Good morning, sir. Good morning and thank you, Chairman Duncan and Congressman O'Rourke and the other distinguished Members of the subcommittee.

My name is Eric Patterson and I am the director of the Federal Protective Service within the National Protection and Programs Directorate of the Department of Homeland Security. I am honored to testify before this committee today regarding the mission and operations of the Federal Protective Service.

In the United States, Government facilities remain a potential target of attacks. FPS's mission is to protect over 9,000 Federal facilities and over 1.4 million occupants and visitors.

To accomplish our mission, FPS inspectors and contract protective security officers, referred to as PSOs, work in tandem to attend to daily security needs at Federal facilities and respond to threats directed against the facilities or the Government personnel working within them.

PSOs are the eyes and ears of our organization. PSOs are responsible for controlling access to Federal facilities, detecting and reporting criminal acts, and responding to emergency situations.

PSOs also ensure prohibited items such as firearms, explosives, knives, and drugs do not enter Federal facilities. In fact, FPS PSOs stop approximately 700,000 prohibited items from entering Federal facilities annually.

All PSOs must undergo preliminary background investigation checks to determine their fitness to begin work on behalf of the Federal Government.

FPS partners with private-sector guard companies to ensure that the guards have met the certification, training, and qualification requirements specified in the contracts, covering subject areas such as ethics, crime scene protection, actions to take in special situations such as building evacuations, safety in fire prevention, and public relations.

To ensure high performance of our contractor PSO force, FPS law enforcement personnel conduct PSO post-inspections and integrate covert test activities to monitor vendor compliance and countermeasure effectiveness. Additionally, vendor files are audited periodically to validate the PSO certifications and training records reflect compliance with contract requirements. In fiscal year 2013 alone, FPS conducted 54,000 post inspections and 17,000 PSO personnel file audits.

As Members of the committee may be aware, the GAO has in the past raised some concerns regarding FPS's handling of PSO train-

ing and oversight. FPS has taken significant steps to improve oversight of PSO contracts.

For example, FPS is currently hiring 39 additional contract officer representatives in order to improve oversight of vendor contract compliance. FPS has also drafted and is vetting an enhanced policy for FPS PSO contract performance monitoring and oversight.

Due in part to these actions, FPS has made significant progress toward closing GAO and OIG recommendations pertaining to our oversight.

FPS also directly employs 1,000 Federal law enforcement personnel who perform a variety of critical functions, including PSO oversight, facility security assessments, and uniformed police response.

To assist our law enforcement personnel in performing oversight of PSO posts, FPS has partnered with DHS Science and Technology to develop a near-term, real-time post-tracking system, also referred to as PTS, which will facilitate the identification of the most effective and efficient solutions for managing our guard force.

One of the most important responsibilities of FPS law enforcement personnel is conducting facility security assessments, also referred to as FSAs. FSAs document security-related risk to a facility and provide a record of countermeasure recommendations designed to enable tenant agencies to meet inter-agency security committee standards for Federal facility security.

Specifically, FPS conducts multiple interviews and in-depth research to support the accomplishment of facility-specific threat assessments. These assessments are an integral first step in establishing the foundation for the risk framework.

FPS collaboration with private sector and Government stakeholders is critical to the successful implementation and characterization of a risk-management framework for each unique facility.

Finally, FPS officers respond to tens of thousands of calls for service annually, which entail responding to criminal activity in progress, to protect life and property, and to respond to National security events or to support other law enforcement responding to a critical situation, as was in the case at the Navy Yard on September 16, 2013.

With regard to responding to an active-shooting incident, I would like to take this opportunity to note that FPS does administer an active-shooter tenant awareness training program and has provided training to more than 3,300 Federal facility tenants. Additionally, while FPS PSOs are not sworn Federal law enforcement officers and are statutorily limited in the scope of actions that they can take during an active-shooter incident, FPS does provide them instruction regarding actions to take in special situations such as a building fire or report of workplace violence or other emergency situations or evacuations.

In closing, I would like to acknowledge and thank our partners, especially members of the law enforcement community, who responded the day of the Navy Yard shooting. The events of September 16 were both a testament to their dedication and training, and a stark reminder of the critical importance of the mission of the Department of Homeland Security and the Federal Protective Service.

The Federal Protective Service remains committed to providing safety, security, protection, and a sense of well-being to thousands of Federal employees, citizens, and visitors who work and conduct business in our Federal facilities daily.

Thank you again for the opportunity to testify before this committee, and I will be pleased to answer any questions you may have.

[The joint prepared statement of Mr. Patterson and Ms. Durkovich follows:]

JOINT PREPARED STATEMENT OF LEONARD E. PATTERSON AND CAITLIN DURKOVICH

OCTOBER 30, 2013

Thank you Chairman Duncan, Ranking Member Barber, and the distinguished Members of the subcommittee. We are pleased to appear before the committee today to discuss the efforts by the National Protection and Programs Directorate (NPPD) to increase security and resilience at our Nation's Federal facilities. The men and women serving in NPPD have wide-ranging responsibilities, from serving on the front lines of law enforcement to developing standards with stakeholders to conducting training Nation-wide. NPPD works with owners and operators, public safety, and countless others daily to keep the Nation secure. These efforts prepare our partners for steady state and day-to-day activity, but also for large-scale and complex incidents. NPPD builds capabilities among our stakeholders and enhances coordination and planning efforts, so when an incident occurs, our employees and stakeholders are prepared to respond and mitigate future incidents.

In addition to working with public and private-sector partners to enhancing security across the sectors, NPPD provides daily protection at Federal facilities through the Federal Protective Service (FPS), protecting more than 1.4 million tenants and visitors in the facilities, on the grounds, and on property owned, occupied, or secured by the Federal Government. Across the country FPS provides law enforcement and security management services, which include operations and oversight of approximately 12,000 contract Protective Security Officers (PSO), and security countermeasure services for more than 9,000 General Services Administration-owned, -leased, or -operated facilities located across the country and other Federal facilities.

ENSURING THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE

Within NPPD, the Office of Infrastructure Protection (IP) works with public and private-sector partners to increase the security and resilience of critical infrastructure and protect the individuals relying on infrastructure. This includes programs to support critical infrastructure owners and operators in enhancing their facilities' security and resilience and coordinating critical infrastructure sectors.

IP is responsible for overall coordination of the Nation's critical infrastructure security and resilience efforts, including development and implementation of the National Infrastructure Protection Plan (NIPP). The NIPP establishes the framework for integrating the Nation's various critical infrastructure security and resilience initiatives into a coordinated effort. The NIPP provides the structure through which the Department of Homeland Security (DHS), in partnership with Government and industry, implements programs and activities to protect critical infrastructure, promote National preparedness, and enhance incident response. The NIPP is regularly updated to capture evolution in the critical infrastructure risk environment, and DHS is currently updating the NIPP based on requirements set forth in Presidential Policy Directive (PPD) 21.[1]

IP conducts on-site risk assessments of critical infrastructure and shares risk and threat information with State, local, and private-sector partners. In addition to helping critical infrastructure owners and operators become more aware of the risks, hazards, and mitigation strategies, we're also helping them measure and compare their levels of security and resilience and how they can improve. In the last year, we conducted more than 900 vulnerability assessments and security surveys on critical infrastructure to identify potential gaps and provide the owners and operators with options to mitigate those gaps and strengthen security and resilience. In addi-

[1] In February 2013, President Obama issued Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience. PPD–21 advances a National unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. One of the requirements set forth in the policy was for DHS to update the NIPP.

tion to serving owners and operators and Government officials directly, IP supports the development of standards, reports, guidelines, and best practices for civilian Federal facilities through the Interagency Security Committee (ISC).

Interagency Security Committee

The mission of the ISC is to safeguard U.S. civilian facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners. The ISC was created following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995—the deadliest attack on U.S. soil before September 11, 2001 and the worst domestic-based terrorist attack in U.S. history. Following the attack, Executive Order 12977 created the ISC to address "continuing Government-wide security" for Federal facilities in the United States.

ISC standards apply to all civilian Federal facilities in the United States. These include facilities that are Government-owned, -leased, or -managed, to be constructed or modernized, or to be purchased, accounting for more than 399,000 Federally-owned and -leased assets and over 3.35 billion square feet Nation-wide.[2] The ISC is truly an interagency body exhibiting collaboration and communication between 53 Federal agencies and departments.[3] When agencies cannot solve security-related problems on their own, the ISC brings chief security officers and senior executives together to solve continuing Government-wide security concerns. The ISC is responsible for the creation and implementation of numerous standards, guidelines, and best practices for the protection of over 300,000 nonmilitary Federal facilities across the country. This work is based on real-world, present-day conditions and challenges and allows for cost savings by focusing on specific security needs of the agencies.

The ISC is a permanent body with appointed members who often serve multi-year terms. Several have represented their organizations for more than a decade. Leadership of the ISC is provided by the assistant secretary for infrastructure protection, an executive director, as well as 8 standing subcommittees: Steering, Standards, Technology, Convergence, Training, Countermeasures, Design-Basis Threat, and the Chair Roundtable.

FPS is an active participant in the work of the ISC, helping shape standards, guidance, and best practices that enable FPS employees to perform their protection mission with consistency and efficiency. FPS sits on the ISC Steering committee, chairs the Training subcommittee, and has representatives on a number of other ISC committees and working groups, including the Design Basis Threat group, the Countermeasures subcommittee, and others. FPS chaired the working group that authored a "Best Practices for Federal Mobile Workplace Security" document in 2013 that is currently under review, and is also on the Active Shooter-Prevention and Response as well as the PPD–21 and Compliance working groups that are currently meeting. In recent years, FPS has also co-chaired the working groups that produced the *Items Prohibited from Federal Facilities: An ISC Standard and Best Practices for Armed Security Officers in Federal Facilities, 2nd Edition* documents. FPS also serves as the Sector-Specific Agency for the Government Facilities Sector. In this role FPS is responsible for working with various partners—including other Federal agencies; State, local, Tribal, and territorial governments as well as other sectors—to develop and implement the Government facilities sector-specific plan.

Standards and Best Practices for Secure Facilities

The ISC issues standards, reports, guidelines, and best practices to protect approximately 1.2 million Federally-owned buildings, structures, and land parcels more than 2.5 million tenant employees, and millions of visitors each day from harm. The documents developed by the ISC affect all civilian Federal facilities—Government-owned, -leased, to be constructed, modernized, or purchased.

Examples of ISC Standards and Guidelines

- *The Risk Management Process for Federal Facilities Standard*.—Issued August 2013, this ISC Standard defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides an integrated, single source of physical security countermeasures for all non-military Federal facilities. The Standard also provides guidance for customization of the countermeasures for Federal facilities and encompasses the following documents:

[2] The Federal Real Property Council's Fiscal Year 2010 Federal Real Property Report, An Overview of the U.S. Federal Government's Real Property Assets.

[3] Additional information on ISC membership is located in the Appendix.

(1) Facility Security Level Determinations (FSL)—2008;
(2) Physical Security Criteria for Federal Facilities—2010;
(3) Design Basis Threat—2013;
(4) Facility Security Committees—2012;
(5) Use of Physical Security Performance Measures—2009;
(6) Child-Care Centers—Level of Protection Template—2010.

- *Violence in the Federal Workplace: A Guide for Prevention and Response*.—Issued April 2013, these Government-wide procedures for threat assessment, intervention, and response to incidents of workplace violence were developed by the ISC, in conjunction with the Chief Human Capital Officers Council and the National Institutes of Occupational Safety and Health.
- *Occupant Emergency Programs: An ISC Guide*.—Issued March 2013, this guidance outlines the components of an Occupant Emergency Program, including those items that comprise an emergency plan, and defines the basic guidelines/procedures to be used for establishing and implementing an effective occupant emergency program.
- *Items Prohibited From Federal Facilities: An ISC Standard*.—Issued February 2013, this standard establishes a guide-line process for detailing control of prohibited items into Federal facilities, and identifies responsibilities for denying entry to those individuals who attempt to enter with such items.
- *Best Practices for Armed Security Officers in Federal Facilities, 2nd Edition*.—Issued February 2013, this best practice recommends a set of minimum standards to be applied to all contract armed security officers working in Federal facilities.
- *Security Specialist Competencies: An ISC Guideline*.—Issued January 2012, this document provides the range of core competencies Federal Security Specialists should possess to perform their basic duties and responsibilities.
- *Best Practices for Mail Screening and Handling*.—Issued September 2011, this joint ISC-Department of Defense Combating Terrorism Technical Support Office/Technical Support Working Group (CTTSO/TSWG) document provides mail center managers, supervisors, and security personnel with a framework for mitigating risks posed by mail and packages.

The ISC continues to identify new initiatives based on current and emerging threats as well as revise policies which may become outdated. Currently the ISC is working on several new initiatives:

- *Active Shooter—Prevention and Response*.—Streamlining existing Federal guidance and ISC policy on Active Shooter into one cohesive guidance document that agencies housed in non-military Federal facilities can use as a reference to enhance preparedness for an active-shooter incident.
- *Facility Security Plan*.—Utilizing the ISC's Risk Management Process to develop guidance agencies can use to develop a Facility Security Plan.
- *Security Office Staffing*.—Establishing criteria and policies which will inform agencies' staffing of Security Offices.
- *Resource Management*.—Developing guidance to help agencies make the most effective use of resources available for physical security across their portfolio of facilities and examine the use of organizational practices for resource management purposes.
- *Presidential Policy Directive 21 and Compliance*.—Developing security criteria for critical infrastructure supporting mission-essential functions to account for PPD–21 requirements and to create a strategy for compliance.
- *Best Practices for Federal Mobile Workplace Security*.—Analyzing the future impact on physical and cybersecurity policy and practices.

Threats to our critical infrastructure, including Federal facilities, are wide-ranging. Not only are there terrorist threats, like the bombing at the Boston Marathon this past spring, but threats from weather-related events, such as Hurricane Sandy, as well as threats to our cyber infrastructure which may have a direct impact on the security of our Federal buildings. While it's impossible to anticipate every threat, NPPD is taking a holistic approach to create a more resilient infrastructure environment to better handle these challenges, and the work of the ISC exemplifies these efforts. Ensuring our Federal facilities are secure and resilient is a large challenge, but by providing our partners with standards and best practices, law enforcement agencies serving at Federal facilities every day, like the Federal Protective Service, have the tools and resources necessary to mitigate threats.

Active-Shooter Preparedness

Recent events have demonstrated the need to identify measures that can be taken to reduce the risk of mass casualty shootings, improve preparedness, and expand and strengthen on-going efforts intended to prevent future incidents. DHS aims to

enhance preparedness through a "whole community" approach by providing training, products, and resources to a broad range of stakeholders on issues such as active-shooter awareness, incident response, and workplace violence.

FPS has developed an Active-Shooter Tenant Awareness training program and has provided this training to more than 3,300 Federal facility tenants so they may be better equipped to analyze a potential situation and work through concerns, actions, and decisions. In addition, more than 1,000 FPS law enforcement officers and agents have been trained in "Active-Shooter Response Tactics." To date, over 9,700 individuals have viewed DHS's active-shooter webinar, over 7,300 attendees have participated in over 100 active-shooter workshops and exercises Nation-wide, and over 263,400 Americans have taken DHS's "Active Shooter: What You Can Do" course. Each workshop allows participants to "live" an emergency incident and analyze the situation to work through concerns, actions, and decisions. DHS also launched an active-shooter webpage in January 2013, which includes active-shooter training resources for Federal, State, and local partners, as well as the public. Since its launch, the page has been accessed more than 258,000 times. In addition to the training FPS provides to tenants, FPS's PSOs receive instruction regarding actions to take in special situations, such as a building fire, a report of an active shooter or workplace violence, and other emergency situations or evacuations.

ENSURING THE SECURITY AND RESILIENCE OF FEDERAL FACILITIES

In the United States Government facilities remain a potential target of attacks. The NPPD FPS mission is to protect Federal facilities and their occupants and visitors by providing superior law enforcement and protective security services, leveraging the intelligence and information resources of its network of Federal, State, local, Tribal, territorial, and private-sector partners. To accomplish our mission and help prevent incidents like the Navy Yard tragedy from occurring at FPS-protected Federal facilities, our inspectors and PSOs work in tandem to attend to daily security needs at Federal facilities, assess individual Federal facilities' vulnerabilities to both natural and man-made events, and effectively respond to security-related activities and threats directed against the facilities or the Government personnel working within them.

In performing the mission of protecting Federal facilities and persons thereon, we rely on our law enforcement and security authorities found at 40 U.S.C. § 1315; our ability to enter into agreements with State, local, and Tribal law enforcement agencies for purposes of protecting Federal property; the enforcement of Federal Management Regulation sections pertinent to conduct on Federal property under 41 C.F.R., Part 102–74 Subpart C; and our responsibility as a recognized "first responder" for all crimes and suspicious circumstances occurring at GSA-owned or -leased property.

FPS OPERATIONS

FPS contracted PSOs are the eyes and ears of our organization. PSOs are responsible for controlling access to Federal facilities, conducting screening at access points to Federal facilities, enforcing property rules and regulations, detecting and reporting criminal acts, and responding to emergency situations involving facility safety and security. PSOs also ensure prohibited items, such as firearms, explosives, knives, and drugs, do not enter Federal facilities. In fact, FPS PSOs stop approximately 700,000 prohibited items from entering Federal facilities annually.

Suitability

All PSOs must undergo preliminary background investigation checks to determine their fitness to begin work on behalf of the Government. At FPS, preliminary checks consist of a review of the applicant's background investigation questionnaire form as well as automated record checks with the FBI, National Crime Information Center, credit reporting bureaus, and naturalization/citizenship checks, when applicable. If derogatory information cannot be mitigated to allow for a favorable preliminary decision, the background investigation must be completed and favorably adjudicated prior to "Entry On Duty" approval. For PSOs serving in Federal facilities requiring a high-level security clearance, DHS uses the Defense Security Service to adjudicate background investigations.

Training

FPS partners with private-sector guard companies to ensure that PSOs are prepared to accomplish their duties. FPS works with the guard companies to ensure the guards have met the certification, training, and qualification requirements specified in the contracts, covering subject areas such as ethics, crime scene protection, actions to take in special situations such as building evacuations, safety and fire

prevention, and public relations. Courses are taught by FPS, by the contract guard company, or by a qualified third party such as the American Red Cross for CPR. PSOs also receive instruction in areas such as X-Ray and magnetometer equipment, firearms training and qualification, baton qualification, and First-Aid certification. PSOs are required to attend refresher training and they must recertify in weapons qualifications in accordance with Federal and State regulations.

The FPS training team is working closely with industry and Federal partners in an effort to further standardize the PSO training screening station-related training. For example, our trainers work with the U.S. Marshals Service and Transportation Security Administration trainers to incorporate best practices into the base X-Ray, Magnetometer, and Hand-Held Metal Detector training. Additionally, FPS is working closely with the National Association of Security Companies to develop a National Lesson Plan for PSOs that will establish a basic and National training program for all PSOs; this is important to ensure standards are consistent across the Nation. These efforts will further standardize training PSOs receive and will provide for a great capability to validate training and facilitate rapid adjustments to training to account for changes in threat and technological advancements.

Oversight

FPS is committed to ensuring high performance of its contracted PSO workforce. FPS Law Enforcement personnel conduct PSO post inspections and integrated covert test activities to monitor vendor compliance and countermeasure effectiveness. Additionally, vendor files are audited periodically to validate that PSO certifications and training records reflect compliance with contract requirements. In fiscal year 2013, FPS conducted 54,830 PSO post inspections and 17,500 PSO personnel file audits.

In addition, and in accordance with procurement regulation and policy, contract deficiencies and performance issues are documented in the annual Contractor Performance Assessment Report. FPS Headquarters and regional leadership are provided with regular reports to maintain visibility on the status of these important assessments that are also used by agency source selection officials in the procurement process when awarding new PSO contracts.

As Members of the committee may be aware, the GAO has, in the past, raised some concerns regarding FPS's handling of PSO training and oversight. FPS has taken significant steps to improve oversight of PSO contracts. For example, FPS is currently hiring 39 additional Contracting Officer Representatives in order to improve oversight of vendor contract compliance. FPS has also drafted and implemented an enhanced policy for FPS PSO performance monitoring, security force management, and contractor management functions. Among other improvements, this standardizes Nationally the methods and frequencies of PSO post inspections and audits of contractor files.

Due in part to these actions, FPS has made significant progress toward closing GAO and OIG recommendations pertaining to oversight. Since 2011, FPS has successfully closed 13 GAO and 4 OIG recommendations and has submitted closure documentation for 9 additional recommendations. Of these, 2 were successfully closed and 7 are pending GAO's internal review for closure.

LAW ENFORCEMENT PERSONNEL

FPS also directly employs over 1,000 Federal Law Enforcement Personnel who are trained physical security experts. Law Enforcement Personnel perform a variety of critical functions, including conducting comprehensive security assessments of vulnerabilities at facilities, developing and implementing protective countermeasures, and providing uniformed police response and investigative follow-up. As previously noted, Law Enforcement Personnel also conduct PSO guard post inspections on a daily basis as well as Operation Shield activities, which involve deployments of a highly visible array of law enforcement personnel to validate and augment the effectiveness of FPS countermeasures across the protective inventory.[4]

Facility Security Assessments

One of the most important responsibilities of FPS Law Enforcement Personnel is conducting Facility Security Assessments (FSAs) at FPS-protected facilities Nationwide. FSAs document security-related risks to a facility and provide a record of

[4] This includes providing highly-visible law enforcement presence to disrupt terrorist/criminal activity, expand patrol and response operations through increased coverage, demonstrate FPS's commitment to employing the highest standards for the security of Federal facilities and the safety of their occupants; and collect and assimilate data to continually assess and improve FPS's ability to achieve its core mission—to secure facilities and safeguard occupants.

countermeasure recommendations. The process analyzes potential threats toward a facility through a variety of research sources and information. Upon identification of the threats, the process identifies and analyzes vulnerabilities to a particular facility utilizing Protective Measure Indices (PMI). Assessors utilize the Modified Infrastructure Survey Tool (MIST) to document the existing protective posture at a facility and compares how a facility is, or is not, meeting the baseline level of protection for its FSL as set forth in the ISC's Physical Security Criteria for Federal Facilities standard and the ISC's Design Basis Threat report. MIST also compares the disparities identified against the baseline level of protection specified in the ISC standards, thereby operationalizing those standards, and enabling mitigation of the vulnerabilities identified. The FSA report is a historical record and informative report provided to FPS stakeholders to support their decision making in risk mitigation strategies.

FSAs require collaboration between FPS private-sector stakeholders and Government stakeholders. Collaboration between these entities is critical to successful implementation of a risk management framework. FPS partners with all of the stakeholders to identify and gather all necessary information for characterizing the risks to each unique facility. FSA is accomplished on a recurring schedule broken down by FSL.

Law Enforcement Response

FPS officers respond to tens of thousands of calls for service annually, some of which entail responding to criminal activity in progress, others to protect life and property, and still others to respond to National security events or to support other law enforcement responding to a critical situation, as was the case in the Navy Yard complex on September 16, 2013. In this case, FPS responded to the on-scene Navy Yard Unified Command center in a supporting role and deployed six K9 Explosive Detection Dog teams to be staged at the Navy Yard and sweep the Nationals Park parking lot in response to mutual-aid calls from the District of Columbia Metropolitan Police Department and the FBI. Additionally, given the proximity of the FPS-protected U.S. Department of Transportation (DOT) building to the Navy Yard complex, FPS deployed to the DOT building, coordinated a Shelter-in-Place for all occupants, established a secure perimeter around the building, conducted K9 sweeps around the perimeter, and increased uniformed patrol activities at other FPS-protected Federal facilities located within the southeast corridor of the District of Columbia.

COMMITMENT TO SECURING FEDERAL FACILITIES

In closing, we would like to acknowledge and thank our partners in both the public and private sector, especially members of the law enforcement community who responded the day of the Navy Yard shooting. We are grateful for their continued service. The shooting at the Navy Yard on September 16 provided a reminder of the need to ensure our infrastructure is secure and resilient so we can protect our communities, regardless of the threat. We must maintain our partnerships and continue to seek new opportunities to enhance the security and resiliency of our Nation while providing our first responders with the resources and tools they need.

DHS is committed to ensuring our Federal facilities remain safe and secure for employees and visitors. Our employees will continue serving on the front lines at Federal facilities and working behind the scenes to develop standards and supporting law enforcement efforts. Thank you again for the opportunity to testify before this committee. We look forward to answering any questions you may have.

APPENDIX.—INTERAGENCY SECURITY COMMITTEE MEMBERSHIP

Membership in the ISC consists of over 100 senior-level executives from 53 Federal agencies and departments. In accordance with Executive Order 12977, modified by Executive Order 13286, primary members represent 21 Federal agencies. Associate membership is determined at the discretion of the ISC Steering Committee and the ISC Chair. Currently, associate members represent 32 Federal departments.

Primary Members (21)

(1) Assistant to the President for National Security Affairs
(2) Central Intelligence Agency
(3) Department of Agriculture
(4) Department of Commerce
(5) Department of Defense
(6) Department of Education

(7) Department of Energy
(8) Department of Health and Human Services
(9) Department of Homeland Security
(10) Department of Housing and Urban Development
(11) Department of the Interior
(12) Department of Justice
(13) Department of Labor
(14) Department of State
(15) Department of Transportation
(16) Department of the Treasury
(17) Department of Veterans Affairs
(18) Environmental Protection Agency
(19) General Services Administration
(20) Office of Management and Budget
(21) U.S. Marshals Service

Associate Members (32)

(1) Commodity Futures Trading Commission
(2) Court Services and Offender Supervision Agency
(3) Federal Aviation Administration
(4) Federal Bureau of Investigation
(5) Federal Communications Commission
(6) Federal Deposit Insurance Corporation
(7) Federal Emergency Management Agency
(8) Federal Protective Service
(9) Federal Reserve Board
(10) Federal Trade Commission
(11) Government Accountability Office
(12) Internal Revenue Service
(13) National Aeronautics & Space Administration
(14) National Archives & Records Administration
(15) National Capital Planning Commission
(16) National Institute of Building Sciences
(17) National Institute of Standards & Technology
(18) National Labor Relations Board
(19) National Science Foundation
(20) Nuclear Regulatory Commission
(21) Office of the Director of International Intelligence
(22) Office of Personnel Management
(23) Office of the U.S. Trade Representative
(24) Securities and Exchange Commission
(25) Smithsonian Institution
(26) Social Security Administration
(27) U.S. Army Corps of Engineers
(28) U.S. Capitol Police
(29) U.S. Coast Guard
(30) U.S. Courts
(31) U.S. Institute of Peace
(32) U.S. Postal Service

Mr. DUNCAN. Thank you.

The Chairman will now recognize Mr. Marshall to testify.

STATEMENT OF GREG MARSHALL, CHIEF SECURITY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MARSHALL. Chairman Duncan, Congressman O'Rourke, Members of the committee, good morning and thank you for the opportunity to provide testimony on access control for Federal facilities.

I am Greg Marshall, the chief security officer for the U.S. Department of Homeland Security. I am a career official with nearly 30 years of law enforcement experience. The mission of my office is to safeguard the Department's people, property, and information. Accordingly, I am responsible, often in partnership with my colleagues at the Federal Protective Service, for security-related

issues affecting more than 235,000 DHS employees that comprise the Department.

The security oversight and guidance authority of my office applies across the Department. However, operational components play a significant role in managing the facilities which they inhabit, including access. The diverse missions and responsibilities of the Department and the facilities used to meet these missions underscore the challenges involved with the physical security and access control disciplines.

The tragic events of Monday, September 16 at the Navy Yard have placed the issue of physical security, access control, and personnel vetting front and center in the minds of security professionals across the Federal landscape. I need to make clear, however, that security aims to manage risk, not eliminate it. Our job is to do everything we can to keep our employees safe, and in doing so we have the benefit of policies and procedures and processes and technologies, both proven and emerging, to help guide and improve our security programs.

When we consider the security for a Federal facility, including access control, we follow the interagency security community standards. Facilities are assessed for risk and appropriate countermeasures are employed. The outcome of these risk assessments drives the level of protection, to include an appropriate access control posture. A one-size security solution, however, cannot and will not fit all.

For employees to qualify for access to facilities, they must undergo a background investigation to establish suitability or fitness for employment. These investigations are for the most part conducted by OPM. Contractors are screened in a similar process to determine fitness for work on a DHS contract and to also have facility access. Background investigations for suitability and fitness examine character and conduct, past conduct. Based upon all available information, we make an adjudicative decision concerning a person's suitability or fitness for employment or access to classified information.

It is important to note that any background investigation, no matter how rigorous, is no guarantee that all relevant information is known, available, or has been included in the investigation. Also, a background investigation may not reliably predict future behavior. A background investigation is an exercise in risk management, establishing some basic facts, but cannot guarantee any individual's continuing fitness to carry out their duties or to behave in a lawful or safe manner.

Recent improvements in our ability to manage these incidents—these inherent risks and incidents include Homeland Security Presidential Directive 12, which mandated a Government-wide standard for secure and reliable credential to be used when accessing Federal facilities. This credential, also known as a PIV card, represents a marked improvement over legacy identity cards. The background investigation process itself is undergoing major Government-wide reform with phased implementation to begin this fiscal year.

The concept of continuous evaluation has been developed to supplement normal reinvestigation reviews with a process that exam-

ines conduct between the reinvestigation time frames. Relevant security information, like a recent arrest, would become available in near-real time, helping to ensure that Classified information and/or Federal facilities are appropriately safeguarded.

Finally, this administration's recent information sharing and safeguarding initiative, also known as "insider threat," seeks to complement background investigations and continuous evaluation with continuous monitoring. This program will incorporate and analyze data in near-real time from a much broader set of sources. Its focus is the protection of Classified information, but its applicability to suitability and contractor fitness is evident.

To conclude, suitability determinations and access control to Federal facilities remains a work in progress, but is evolving toward dramatic improvement. We have made great progress, but managing employee and facility risks will continue to be a challenge.

Thank you again for the opportunity to testify today.

[The prepared statement of Mr. Marshall follows:]

PREPARED STATEMENT OF GREGORY MARSHALL

OCTOBER 30, 2013

Chairman Duncan, Ranking Member Barber, Members of the committee, good morning and thank you for the opportunity to provide testimony on access control for Federal facilities.

I am Greg Marshall, chief security officer of the U.S. Department of Homeland Security (DHS). I lead the dedicated men and women who make up the Office of the Chief Security Officer. My office is an element of the Department's Management Directorate, and I report to the under secretary for management.

The mission of our office is to safeguard the Department's people, property, information, and systems. Accordingly, the DHS chief security officer, often in partnership with the Federal Protective Service, is responsible for security-related issues affecting the more than 240,000 DHS employees that compose the Department. I exercise DHS-wide security program authorities in the areas of personnel security, physical security, administrative security, special security, identity management, special access programs, and security training and awareness. I also support the chief information officer in the area of IT security policy and the under secretary for intelligence and analysis in the protection of intelligence sources and methods, and accreditations of Classified facilities.

The security oversight and guidance authority of my office applies across the Department. However, Operational components play a significant role in managing the facilities which they inhabit, including access to those facilities. The diverse missions and responsibilities of the Department underscore the challenges involved within the physical security and access control disciplines.

The tragic events of Monday, September 16 at the Washington Navy Yard have placed the issue of physical security, access control, and personnel vetting front and center in the minds of security professionals across the Federal landscape.

Shortly after the Navy yard incident, I convened a meeting of the Department's Chief Security Officer Council. Each component Chief Security Officer (CSO) acknowledged the significance of the Navy Yard tragedy to access control and the underlying vetting processes and each CSO commented on the complexities of vetting and access, including the costs involved. With this in mind, the Department remains committed to ensuring that only those persons with a legitimate need to access any given facility are allowed to enter, that those persons possess no prohibited items, and that the backgrounds of those persons who do enter have been vetted to an appropriate level of rigor.

I would make clear, however, that security involves risk management. Our job is to do everything we can to reduce the risk and keep our employees safe. In pursuit of our mission, please be assured that DHS security leadership and the professionals we manage have the benefit of extensive knowledge, training, and experience. We also have the benefit of comprehensive policies, procedures, processes, and emerging technologies to help guide and improve our key security programs.

For example, when we consider the security posture for a Federal facility, including access control, we at DHS follow Interagency Security Committee standards.

During this process, facilities are assessed for risk, and appropriate countermeasures are employed to mitigate the risks. Using a decision matrix involving mission criticality, the sensitivity of the activities conducted, threats to the facility, facility population of persons who work and visit there, and other factors, an appropriate Federal Security Level is assigned to each facility. Accordingly, the outcomes of these risk assessments drive the level of protection for each facility, to include an appropriate access control posture. Simply put, a one-size security solution does not and cannot fit all facilities.

For our employees to qualify for access to a Federal DHS facility, an employee must undergo a background investigation to establish his or her suitability for employment. These investigations are, for the most part, conducted by OPM on behalf of DHS. Contractors are screened in a process similar to employees in order to determine their fitness to work on a DHS contract and have unescorted access to DHS facilities. Background investigations for suitability and fitness examine character and conduct behaviors, such as criminal history, alcohol and drug use, and employment history, among others. Based upon all available information, a personnel security specialist makes an adjudicative decision concerning a person's suitability or fitness for employment, including access to facilities.

It is important to understand that a background investigation for suitability and one for a security clearance processes with multiple levels of investigation dependent upon the access required and level of risk. A security clearance allows access to Classified information, while a favorable suitability or fitness determination allows employment and access to facilities. On its own, a background investigation for suitability does not permit access to Classified information.

It is also important to note that a background investigation for either a suitability determination or a security clearance, no matter how rigorous, is no guarantee that every bit of relevant information about the individual is available or has been included. For example, prior criminal convictions and/or arrest information may not be reported in State and/or Federal repositories, often simply due to data entry resource constraints. It is these types of checks that are basic elements of any Federal employment background investigation.

Also, it is important to note that a background investigation may not be an indicator of future behavior. Even those who have successfully undergone the most rigorous set of background checks available—even a comprehensive polygraph examination—may someday prove untrustworthy. Ultimately, a Federal background investigation only examines past behavior and is sometimes based on limited available information.

A Federal background investigation is an exercise in risk management, establishing some basic facts such as identity, citizenship, criminal history, etc. However, a background investigation cannot be characterized, in and of itself, does not guarantee any single individual's continuing day-to-day fitness to carry out his or her employment responsibilities or to behave in a lawful and safe manner.

With these limitations in mind, there have been several recent improvements to the ability of the Government to manage these inherent risks.

First, Homeland Security Presidential Directive 12 (HSPD–12) mandated the development and implementation of a Government-wide standard for a secure and reliable Personal Identity Verification (PIV) card for gaining access to Federally-controlled facilities. To date, DHS Headquarters and components have issued over 250,000 PIV cards to Federal employees and contractors. For the first time, this process has effectively linked the completion of a person's background investigation with the issuance to that person of a unique Federal identity credential. The PIV card represents a marked improvement over the various legacy access/identity cards, but is only a part of any solution. As a result, Federal facility access control processes use this PIV card and its various authentication mechanisms to verify the identity of the holder, link the holder to the card, and link the card itself to a database of valid employees and contractors having legitimate business at any given facility.

Second, the background investigation process itself is undergoing a major Government-wide reform effort, to include revised Federal investigative standards signed jointly by the director of National Intelligence and the director of the Office of Personnel Management in 2012, and phased implementation to begin this fiscal year. With the Federal investigative standards, the concept of "continuous evaluation" is being developed to supplement the normal re-investigation reviews of employees which, under the revised standards, will be in 5-year increments, with a Government-led process that examines a person's conduct within his or her normal re-investigation time frames. As such, relevant security information like a recent arrest or conviction for a crime outside of the Federal system, for example, would become available on a timelier basis to security officials responsible for assessing a person's

eligibility for access to Classified information, thereby helping to ensure that Classified information and/or Federal facilities are appropriately safeguarded. "Continuous evaluation" represents a significant process improvement over current capabilities and will mitigate some of the limitations in the existing background investigation process discussed above.

Finally, this administration's recent Information Sharing and Safeguarding initiative, also known as "Insider Threat," seeks to complement background investigations and continuous evaluation with continuous monitoring. Continuous monitoring will incorporate data in near-real time from a much broader set of data sources, as compared to information that was previously available in the background investigation process. The initiative focuses on monitoring certain IT systems and incorporates analysis and collation software to aid in the identification of behavioral trends that could be indicative of an insider threat problem. Strict referral protocols are in place to investigate abnormalities. The aim is the detection and mitigation of threats to Classified information before any damage can be done. The focus of this program is the protection of Classified information, but its applicability to other behavioral issues, including suitability and contractor fitness, is evident.

In conclusion, the suitability determinations of and access control to Federal facilities by Federal employees and contractors remains a work in progress, but is evolving toward dramatic improvement. It is our responsibility as DHS security leaders, with the support of Congress, to ensure a safe and secure workplace. We have made important strides, but assessing and managing employee and facility risks will continue to be a challenge in the future. We will continue to work every day to meet these challenges. Thank you again for the opportunity to testify today.

Mr. DUNCAN. Thank you so much, Mr. Marshall.

Ms. Durkovich. If I pronounced that wrong, just tell me—Durkovich?

Ms. DURKOVICH. You have pronounced it correctly. Thank you, sir.

Mr. DUNCAN. Thank you so much. You are recognized for 5 minutes.

STATEMENT OF CAITLIN DURKOVICH, ASSISTANT SECRETARY, INFRASTRUCTURE PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY, TESTIFYING ON BEHALF OF THE INTERAGENCY SECURITY COMMITTEE

Ms. DURKOVICH. Thank you very much, Chairman Duncan and Ranking Member O'Rourke and the distinguished Members of the subcommittee. I am honored to appear before you today.

As assistant secretary for infrastructure protection, I have the responsibility to lead the overall coordination of the Nation's critical infrastructure security and resilience efforts, including development and implementation of the National Infrastructure Protection Plan, or the NIPP. The NIPP establishes the framework for integrating the Nation's various critical infrastructure security and resilience initiatives into a coordinated effort.

One of the most rewarding opportunities I have is to serve as chair of the Interagency Security Committee and oversee the development of standards and guidelines and best practices for civilian Federal facilities through the Interagency Security Committee, or the ISC. The ISC was created by Executive Order following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995.

The ISC is responsible for the creation and adoption of numerous standards, guidelines, and best practices for the protection of nearly 400,000 non-military Federal facilities across the country. This work is based on real-world present-day conditions and challenges

and allows for cost savings by focusing on specific security needs of the agencies.

ISC standards provide the Federal community with strategies for identifying physical security measures and support the design and implementation of risk-based security policies. In August, the ISC issued the risk management process for Federal facilities standard, which defines the criteria and processes that those responsible for security should use to determine a facility's security level and provides an integrated single source of physical security countermeasures for all non-military Federal facilities.

The standard also provides guidance for customization of countermeasures for Federal facilities and explains that risk can be addressed in various ways, depending on agency mission needs, for example, the presence of child care on-site and historical significance. It is most important to note that the ISC is truly a collaborative interagency body. Fifty-three Federal departments and agencies participate in the ISC and take the lead on bringing ideas to the table and drafting standards and best practices.

When agencies cannot solve security-related problems on their own, the ISC is a convening body for chief security officers and senior executives to solve continuing Government-wide security concerns. The ISC membership develops standards and best practices based on real-world threats. Recent events have demonstrated the need to identify measures that can be taken to reduce the risk of mass-casualty shootings, improve preparedness, and expand and strengthen on-going efforts intended to prevent future incidents.

DHS aims to enhance preparedness through a whole-of-community approach, by providing resources to a broad range of stakeholders on issues such as active-shooter awareness, incident response, and workplace violence.

Working with partners in the private sector, DHS developed training and other awareness materials to assist critical infrastructure owners and operators with better training their staff and coordinating with local law enforcement.

We have hosted hundreds of workshops and developed an on-line training tool targeted at preparing those who work in these buildings.

These efforts and resources have been well-received and are applicable to Government facilities as well as commercial spaces.

Cognizant of this growing threat, the ISC this past spring formed a Federal active-shooter working group. While a number of Federal guidance documents previously existed on active-shooter preparedness and response, including our designed basis threat report, the violence in Federal workplace, a guide for prevention response, and occupant emergency programs, an ISC guide, the working group was formed to streamline existing ISC policies into a single cohesive document.

To date, the working group has met four times and has reviewed numerous publications and guidance documents, including training materials developed by the Department for commercial facilities.

It will also leverage lessons learned from real-world incidents, including the Navy Yard shooting.

It is our intention that the resulting work will serve as a resource for agencies to enhance preparedness for an active-shooter incident in a Federal facility.

Threats to our critical infrastructure, including Federal facilities, are wide-ranging. Not only are there terrorist threats, like the bombing at the Boston Marathon this past spring, or the complex shopping mall attack we saw recently overseas, but threats from weather-related events, such as Hurricane Sandy, as well as threats to our cyber infrastructure which may have a direct impact on the security of our Federal buildings.

While it is impossible to anticipate every threat, the Department is taking a holistic approach to create a more secure and resilient infrastructure environment to better handle these challenges, and the work of the ISC exemplifies these efforts.

Ensuring our Federal facilities are secure and resilient is a large undertaking. But the work of our 53 member departments and agencies to ensure those responsible for Federal facility security have the tools and resources necessary to mitigate these threats is worth noting.

In closing, I would like to thank you for the opportunity to appear before you and discuss the important work of the ISC. I look forward to answering any questions you may have.

Mr. DUNCAN. Thank you so much.

The Chairman will now recognize Mr. Goldstein for 5 minutes.

STATEMENT OF MARK L. GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. GOLDSTEIN. Good morning, Mr. Chairman and Members of the subcommittee. We are pleased to be here today to discuss our latest report on the Federal Protective Service and the protection of Federal facilities.

As part of the Department of Homeland Security, the FPS is responsible for protecting Federal employees and visitors in approximately 9,600 Federal facilities.

Sadly, recent incidents at Federal facilities demonstrate their continued vulnerability to attacks and other acts of violence.

To help accomplish its mission, FPS conducts the facility risk assessments and provides oversight of approximately 13,500 contract security guards deployed to Federal facilities.

My testimony today is based on the results of a September 2013 report which is being released by the subcommittee today, previous GAO reports on this topic and the preliminary results of work GAO conducted for a report that we will issue to the Chairman later this year.

My testimony today discusses challenges FPS faces in ensuring contract security guards deployed to Federal facilities are properly trained and certified, and the extent to which FPS and select Federal agencies' facility risk assessment methodologies align with standards issued by the ISC.

Our findings are as follows: First, the Federal Protective Service faces challenges ensuring that contract guards have been properly trained and certified before being deployed to Federal facilities.

In particular, GAO found that providing active-shooter response and screener training is a challenge for FPS. For example, according to officials at five guard companies, their contract guards have not received training on how to respond during incidents involving an active shooter.

Without ensuring that all guards receive this training, FPS has limited assurance that its guards are prepared for such a threat. Similarly, officials from one of FPS' contract guard companies stated that 133, about 38 percent of its approximately 350 guards, had never received screener training. As a result, those guards may be using X-ray and magnetometer equipment at Federal facilities that they are not qualified to use, raising questions about their ability to properly screen access control points at Federal facilities, one of their primary responsibilities.

We were unable to determine the extent to which FPS' guards have received active-shooter response and screener training.

Second, GAO also found that FPS continues to lack effective management controls to ensure its guards have met its training and certification requirements.

For instance, although FPS agreed with GAO's 2010 and 2012 recommendations that it develop a comprehensive and reliable system for managing information on guard's training, certifications, and qualifications, it still does not have such a system.

Additionally, 23 percent of nearly 300 guard files that GAO examined, maintained by 11 of the 31 contract guard companies we interviewed, lacked required training and certification documents. Examples of missing items include documentation of initial weapons and screener training and firearms qualifications.

Finally, GAO's preliminary results on our risk assessment report indicate that several agencies, including FPS, do not use a methodology to assess risk at their facilities that aligns with the ISC's risk assessment standards.

Risk assessments help decision makers identify and evaluate security risks and implement protective measures to mitigate risk. ISC's standards state that agencies' facility risk assessment methodologies must, first, consider all of the undesirable events identified by ISC as a possible risk to Federal facilities, and, No. 2, assess the threat vulnerability and consequences of specific undesirable events.

Most commonly, FPS and eight agencies' methodologies that we reviewed are inconsistent with ISC standards because they do not assess facilities' vulnerabilities to specific undesirable events. If an agency does not know its facility's potential vulnerabilities to specific scenarios, it cannot set priorities to mitigate these vulnerabilities.

In addition, as GAO reported in August 2012, although Federal agencies pay FPS millions of dollars to assess risk at their facilities, FPS' own risk assessment tool is not consistent with ISC's risk assessment standards, because it does not assess consequence, the level, duration, and nature of loss, resulting from undesirable events.

As a result, FPS and the agencies we reviewed may not have a complete understanding of the risks facing approximately 57,000 Federal facilities located around the country, including the 9,600

facilities that FPS protects. As mentioned, our final report on this topic will be available later this fall.

Mr. Chairman, this completes my statement. I would be happy to respond to any questions. Thank you.

[The prepared statement of Mr. Goldstein follows:]

PREPARED STATEMENT OF MARK L. GOLDSTEIN

OCTOBER 30, 2013

GAO HIGHLIGHTS

Highlights of GAO–14–128T, a testimony before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

As part of the Department of Homeland Security (DHS), FPS is responsible for protecting Federal employees and visitors in approximately 9,600 Federal facilities under the control and custody of the General Services Administration (GSA). Recent incidents at Federal facilities demonstrate their continued vulnerability to attacks or other acts of violence. To help accomplish its mission, FPS conducts facility risk assessments and provides oversight of approximately 13,500 contract security guards deployed to Federal facilities.

This testimony is based on the results of our September 2013 report (released by the subcommittee today), previous reports, and preliminary results of work GAO conducted for a report that GAO plans to issue to the Chairman later this year. GAO discusses: (1) Challenges FPS faces in ensuring contract security guards deployed to Federal facilities are properly trained and certified, and (2) the extent to which FPS and select Federal agencies' facility risk assessment methodologies align with standards issued by the ISC. To perform this work, GAO reviewed FPS and guard company documentation and interviewed officials about oversight of guards. GAO also reviewed FPS's and 8 Federal agencies' risk assessment documentation and compared it to ISC's standards. These agencies were selected based on their missions and types of facilities.

What GAO Recommends

DHS and FPS agreed with GAO's recommendations in its September 2013 report.

HOMELAND SECURITY.—CHALLENGES ASSOCIATED WITH FEDERAL PROTECTIVE SERVICE'S CONTRACT GUARDS AND RISK ASSESSMENTS AT FEDERAL FACILITIES

What GAO Found

The Federal Protective Service (FPS) faces challenges ensuring that contract guards have been properly trained and certified before being deployed to Federal facilities around the country. In a September 2013 report, GAO found that providing active-shooter response and screener training is a challenge for FPS. For example, according to officials at five guard companies, their contract guards have not received training on how to respond during incidents involving an active shooter. Without ensuring that all guards receive this training, FPS has limited assurance that its guards are prepared for such a threat. Similarly, officials from one of FPS's contract guard companies stated that 133 (about 38 percent) of its approximately 350 guards have never received screener training. As a result, those guards may be using X-ray and magnetometer equipment at Federal facilities that they are not qualified to use, raising questions about their ability to properly screen access control points at Federal facilities—one of their primary responsibilities. We were unable to determine the extent to which FPS's guards have received active-shooter response and screener training. FPS agreed with GAO's 2013 recommendation that they take steps to identify guards that have not had required training and provide it to them. GAO also found that FPS continues to lack effective management controls to ensure its guards have met its training and certification requirements. For instance, although FPS agreed with GAO's 2010 and 2012 recommendations that it develop a comprehensive and reliable system for managing information on guards' training, certifications, and qualifications, it still does not have such a system. Additionally, 23 percent of the 276 guard files GAO examined (maintained by 11 of the 31 guard companies we interviewed) lacked required training and certification documentation. Examples of missing items include documentation of initial weapons and screener training and firearms qualifications.

GAO's preliminary results indicate that several agencies, including FPS, do not use a methodology to assess risk at their facilities that aligns with the Interagency Security Committee's (ISC) risk assessment standards. Risk assessments help decision makers identify and evaluate security risks and implement protective measures to mitigate the risk. ISC's standards state that agencies' facility risk assessment methodologies must: (1) Consider all of the undesirable events identified by ISC as possible risks to Federal facilities, and (2) assess the threat, vulnerability, and consequence of specific undesirable events. Most commonly, agencies' methodologies that GAO reviewed are inconsistent with ISC's standards because they do not assess facilities' vulnerabilities to specific undesirable events. If an agency does not know its facilities' potential vulnerabilities to specific undesirable events, it cannot set priorities to mitigate these vulnerabilities. In addition, as GAO reported in August 2012, although Federal agencies pay FPS millions of dollars to assess risk at their facilities, FPS's risk assessment tool is not consistent with ISC's risk assessment standards because it does not assess consequence (i.e., the level, duration, and nature of loss resulting from undesirable events). As a result, FPS and the other noncompliant agencies GAO reviewed may not have a complete understanding of the risks facing approximately 57,000 Federal facilities located around the country (including the 9,600 protected by FPS).

Chairman Duncan, Ranking Member Barber, and Members of the subcommittee: We are pleased to be here to discuss the results of our September 2013 report, which the subcommittee is releasing today, and the efforts of the Department of Homeland Security's (DHS) Federal Protective Service (FPS) to protect the nearly 9,600 Federal facilities that are under the control and custody of the General Services Administration (GSA). The 2012 shooting at the Anderson Federal Building in Long Beach, California, and the results of our 2009 covert testing and FPS's ongoing penetration testing demonstrate the continued vulnerability of Federal facilities. Moreover, the challenge of protecting Federal facilities is one of the major reasons why we have designated Federal real property management as a high-risk area.[1]

FPS is authorized: (1) To protect the buildings, grounds, and property that are under the control and custody of GSA, as well as the persons on the property; (2) to enforce Federal laws and regulations aimed at protecting such property and persons on the property; and (3) to investigate offenses against these buildings and persons.[2] FPS conducts its mission by providing security services through two types of activities: (1) Physical security activities—conducting security assessments and recommending countermeasures aimed at preventing incidents—and, (2) law enforcement activities—proactively patrolling facilities, responding to incidents, conducting criminal investigations, and exercising arrest authority. To accomplish its mission, FPS currently has almost 1,200 full-time employees and about 13,500 contract guards deployed at Federal facilities across the country. It expects to receive approximately $1.3 billion in fees for fiscal year 2013.[3]

Since 2008, we have reported on the challenges FPS faces with carrying out its mission, including overseeing its contract guards and assessing risk at Federal facilities. FPS's contract guard program is the most visible component of the agency's operations, and the agency relies on its guards to be its "eyes and ears" while performing their duties. However, we reported in 2010 and again in 2013 that FPS continues to experience difficulty ensuring that its guards have the required training and certifications. Before guards are assigned to a post (an area of responsibility) at a Federal facility, FPS requires that they all undergo employee fitness determinations[4] and complete approximately 120 hours of training provided by the contractor and FPS, including basic training and firearms training. Among other duties, contract guards are responsible for controlling access to facilities; conducting screening at access points to prevent the introduction of prohibited items, such as weapons and explosives; and responding to emergency situations involving facility safety and

---

[1] GAO, *High Risk Series: An Update,* GAO–13–283 (Washington, DC: Feb. 14, 2013).

[2] Section 1315(a) of title 40, United States Code, provides that: "To the extent provided for by transfers made pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security . . . shall protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property."

[3] To fund its operations, FPS charges fees for its security services to Federal tenant agencies in GSA-controlled facilities.

[4] A contractor employee's fitness determination is based on the employee's suitability for work for or on behalf of the Government based on character and conduct.

security.[5] FPS also faces challenges assessing risks at the 9,600 facilities under the control and custody of GSA. For instance, in 2012, we reported that FPS's ability to protect and secure Federal facilities has been hampered by the absence of a risk assessment program that is consistent with Federal standards.

This testimony is based on our September 2013 report, released today,[6] previous reports,[7] and preliminary results of work we conducted for a report that we plan to issue to the Chairman later this year.[8] This testimony discusses: (1) Challenges FPS faces in ensuring contract security guards deployed to Federal facilities are properly trained and certified, and (2) the extent to which FPS and select Federal agencies' facility risk assessment methodologies align with Federal risk assessment standards issued by the Interagency Security Committee (ISC).[9] To identify challenges associated with ensuring FPS's contract guards are properly trained and certified, we analyzed selected guard services contracts active as of September 2012 and FPS's Security Guard Information Manual. We drew a non-generalizable sample of 31 contracts from FPS's 117 guard services contracts (one contract for every guard company with which FPS has contracted for non-emergency guard services).[10] A subset (11) of the 31 guard contracts was chosen based on geographic diversity and geographic density of contracts within FPS regions to allow us to conduct file reviews for multiple contracts during each of four site visits that we conducted. For each of these 11 contracts, we reviewed the contracts as well as a random sample of guard files associated with each contract. The remaining 20 guard services contracts we selected were the most recent contract for each of the remaining guard companies that FPS had contracted with as of November 2012. We also interviewed officials from each of the 31 contract guard companies.

To determine the extent to which contract guard companies documented compliance with FPS's guard training and certification requirements, we examined documentation related to our non-generalizeable sample of 11 contracts, as previously discussed. From these 11 contracts, we randomly selected 276 guard files to review for compliance with FPS requirements. For each guard file, we compared the file documents to a list of requirements contained in FPS's Administrative Audit and Protective Security Officer File Review Forms, which FPS uses to conduct its monthly guard file reviews.

To identify the management controls and processes FPS and the guard companies use to ensure compliance with training, certification, and qualification requirements, we reviewed FPS's procedures for: (1) Conducting monthly guard file reviews; (2) documenting compliance with guard training, certification, and qualification requirements; and (3) monitoring performance. We also visited 4 of FPS's 11 regions to discuss how regional officials ensure that guards are qualified to be deployed to Federal facilities. We selected the 4 regions to provide geographic density of contracts in the region to facilitate reviews of guard files, diversity in the size of guard companies, and geographic diversity. In addition, we interviewed officials from each of FPS's 31 guard companies regarding their policies and procedures for complying with FPS's guard training and certification requirements. While the results of our work are not generalizeable, about 40 percent of the GSA facilities with guards are located in the four regions where we conducted our site visits and our review of

---

[5] In general, guards may only detain, not arrest, individuals at their facility. Some guards may have arrest authority under conditions set forth by the individual States.

[6] GAO, *Federal Protective Service: Challenges with Oversight of Contract Guard Program Still Exist, and Additional Management Controls Are Needed,* GAO–13–694 (Washington, DC: September 2013).

[7] GAO, *Federal Protective Service: Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities,* GAO–12–739 (Washington, DC: August 2012), GAO, *Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards,* GAO–10–341 (Washington, DC: April 2010), and GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities,* GAO–08–683 (Washington, DC: June 2008).

[8] That report will contain our final evaluation and recommendations about agencies' risk assessment methodologies.

[9] The Interagency Security Committee (ISC) was created pursuant to Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 19, 1995), as amended by Executive Order 13286, 68 Fed. Reg. 10610 (March 5, 2003). The ISC is a permanent body established to address continuing Government-wide security for Federal facilities and was tasked with, among other things, developing security standards for Federal facilities. The ISC is comprised of primary members from Federal Executive branch agencies designated by the Executive Order as well as associate members from other agencies and departments not designated in the Executive Order. The ISC is to be chaired by the Secretary of DHS or a designee of the Secretary.

[10] When we chose contracts for review, FPS had a total of 117 contracts with 32 guard companies. However, 1 of the 32 companies had a contract with FPS for only emergency guard services. As such, we chose 1 contract for review for each company with which FPS had contracted for non-emergency guard services as of November 2012.

guard files involved 11 of FPS's 31 guard companies. To assess the extent to which FPS's monthly guard-file review results identified files with missing documentation of training, certifications, and qualifications, we compared FPS's monthly file review results from the month in which we conducted our file review for each of the 11 contracts to identify guard files that were included in both our review and FPS's monthly review. We identified any discrepancies between the reviews and used FPS's file review forms to examine the discrepancies.

To determine the extent to which FPS and select Federal agencies' facility risk assessment methodologies align with ISC's risk assessment standards, we reviewed and analyzed risk assessment documentation and interviewed officials at 9 Federal agencies and compared each agency's methodology to ISC's standards. The nine selected agencies include: Department of Energy, Office of Health, Safety, and Security; Department of Interior; Department of Justice, Justice Protective Service; Department of State, Diplomatic Security; Department of Veterans Affairs; Federal Emergency Management Agency; Federal Protective Service; Nuclear Regulatory Commission; and Office of Personnel Management. These agencies were selected to achieve diversity with respect to the number and types of agencies' facilities, as well as the agencies' missions.

We conducted our on-going work from August 2012 to October 2013 in accordance with generally accepted Government auditing standards. Also, our previously-issued reports were done in accordance with these 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.

FPS FACES CHALLENGES ENSURING CONTRACT GUARDS HAVE BEEN PROPERLY TRAINED AND CERTIFIED BEFORE BEING DEPLOYED TO FEDERAL FACILITIES

Some FPS Contract Guards Have Not Received Required Training on Responding to Active-Shooter Scenarios

According to FPS officials, since 2010 the agency has required its guards to receive training on how to respond to an active-shooter scenario. However, as our 2013 report shows,[11] FPS faces challenges providing active-shooter response training to all of its guards. According to FPS officials, the agency provides guards with information on how they should respond during an active-shooter incident as part of the 8-hour FPS-provided orientation training. FPS officials were not able to specify how much time is devoted to this training, but said that it is a small portion of the 2-hour special situations training.[12] According to FPS's training documents, this training includes instructions on how to notify law enforcement personnel, secure the guard's area of responsibility, appropriate use of force, and direct building occupants according to emergency plans.

However, when we asked officials from 16 of the 31 contract guard companies we spoke to if their guards had received training on how guards should respond during active-shooter incidents, responses varied.[13] For example, of the 16 contract guard companies we interviewed about this topic:

- officials from 8 contract guard companies stated that their guards have received active-shooter scenario training during FPS orientation;
- officials from 5 guard companies stated that FPS has not provided active-shooter scenario training to their guards during the FPS-provided orientation training; and,
- officials from 3 guard companies stated that FPS had not provided active-shooter scenario training to their guards during the FPS-provided orientation training, but that the topic was covered at some other time.

We were unable to determine the extent to which FPS's guards have received active-shooter response training. Without ensuring that all guards receive training on how to respond to active-shooter incidents, FPS has limited assurance that its guards are prepared for this threat. FPS agreed with our recommendation that they take immediate steps to determine which guards have not received this training and provide it to them.

---

[11] GAO–13–694.

[12] This training is provided during a block of training on special situations, which includes information on how guards should respond to situations other than their normal duties, such as reports of missing or abducted children, bomb threats, and active-shooter scenarios. FPS officials stated that guards hired before 2010 should have received this information during guard-company-provided training on the guards' post orders (which outline the guards' duties and responsibilities) as part of basic and refresher training.

[13] The remaining 15 guard companies did not respond to this question.

Some FPS Guards Have Not Received Required Screener Training

As part of their 120 hours of training, guards must receive 8 hours of screener training from FPS on how to use X-ray and magnetometer equipment. However, in our September 2013 report,[14] we found that FPS has not provided required screener training to all guards. Screener training is important because many guards control access points at Federal facilities and thus must be able to properly operate X-ray and magnetometer machines and understand their results. In 2009 and 2010, we reported that FPS had not provided screener training to 1,500 contract guards in one FPS region.[15] In response to our reports, FPS stated that it planned to implement a program to train its inspectors to provide screener training to all of its contract guards. However, 3 years after our 2010 report, guards continue to be deployed to Federal facilities who have never received this training. For example, an official at one contract guard company stated that 133 of its approximately 350 guards (about 38 percent) on three separate FPS contracts (awarded in 2009) have never received their initial X-ray and magnetometer training from FPS. The official stated that some of these guards are working at screening posts. Further, officials at another contract guard company in a different FPS region stated that, according to their records, 78 of 295 (about 26 percent) guards deployed under their contract have never received FPS's X-ray and magnetometer training. These officials stated that FPS's regional officials were informed of the problem, but allowed guards to continue to work under this contract, despite not having completed required training. Because FPS is responsible for this training, according to guard company officials no action was taken against the company. Consequently, some guards deployed to Federal facilities may be using X-ray and magnetometer equipment that they are not qualified to use—thus raising questions about the ability of some guards to execute a primary responsibility to properly screen access control points at Federal facilities. We were unable to determine the extent to which FPS's guards have received screener training. FPS agreed with our recommendation that they take immediate steps to determine which guards have not received screener training and provide it to them.

FPS Lacks Effective Management Controls to Ensure Guards Have Met Training and Certification Requirements

In our September 2013 report, we found that FPS continues to lack effective management controls to ensure that guards have met training and certification requirements. For example, although FPS agreed with our 2010 and 2012 recommendations to develop a comprehensive and reliable system for contract guard oversight, it still does not have such a system. Without a comprehensive guard management system, FPS has no independent means of ensuring that its contract guard companies have met contract requirements, such as providing qualified guards to Federal facilities. Instead, FPS requires its guard companies to maintain files containing guard-training and certification information and to provide it with a monthly report containing this information. In our September 2013 report, we found that 23 percent of the 276 guard files we reviewed (maintained by 11 of the 31 guard companies we interviewed) lacked required training and certification documentation.[16] As shown in Table 1, some guard files lacked documentation of basic training, semi-annual firearms qualifications, screener training, the 40-hour refresher training (required every 3 years), and CPR certification.

TABLE 1.—TOTAL MISSING DOCUMENTS IDENTIFIED IN 64 OF 276 GUARD FILES GAO REVIEWED

Requirement	Number of Instances of Each Missing Document
Copy of driver's license/State ID	1
Domestic Violence "Lautenberg" Form	1
Medical certification	1
Verified alien/immigration status	3

[14] GAO–13–694.

[15] GAO, *Homeland Security: Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist,* GAO–09–1047T (Washington, DC: Sept. 23, 2009) and GAO–10–341.

[16] See GAO–13–694. During our non-generalizeable review of 276 randomly-selected guard files, we found that 64 files (23 percent) were missing one or more required documents.

TABLE 1.—TOTAL MISSING DOCUMENTS IDENTIFIED IN 64 OF 276 GUARD FILES GAO REVIEWED—Continued

Requirement	Number of Instances of Each Missing Document
Current baton certification	3
Basic training	3
Firearms qualifications	3
First-aid certification	5
FPS screener training—8 hours	5
FPS orientation	8
Contractor employee fitness determination	12
CPR certification	12
AED certification	12
Refresher training	15
Pre-employment drug testing	16
Initial weapons training	17
Total	[1] 117

Source.—GAO analysis of contract guard company data.

Note.—These results are non-generalizeable and based on a review of 276 randomly-selected guard files for 11 of 117 FPS guard contracts.

[1] Some of the files that did not comply with requirements were missing more than one document, for a total of 117 missing documents.

FPS has also identified guard files that did not contain required documentation. FPS's primary tool for ensuring that guard companies comply with contractual requirements for guards' training, certifications, and qualifications is to conduct monthly reviews of guard companies' guard files. From March 2012 through March 2013, FPS reviewed more than 23,000 guard files.[17] It found that a majority of the guard files had the required documentation but more than 800 (about 3 percent) did not. FPS's file reviews for that period showed files missing, for example, documentation of screener training, initial weapons training, CPR certification, and firearms qualifications. However, as our September 2013 report explains, FPS's process for conducting monthly file reviews does not include requirements for reviewing and verifying the results, and we identified instances in which FPS's monthly review results did not accurately reflect the contents of guard files. For instance, FPS's review indicated that required documentation was present for some guard files, but we were not able to find documentation of training and certification, such as initial weapons training, DHS orientation, and pre-employment drug screenings.[18] As a result of the lack of management controls, FPS is not able to ensure that guards have met training and certification requirements.

GAO's Recommendations to Improve the Management and Oversight of FPS's Contract Guard Program

In our September 2013 report, we recommended that DHS and FPS take the following actions:

- take immediate steps to determine which guards have not had screener or active-shooter scenario training and provide it to them and, as part of developing a National curriculum, decide how and how often these trainings will be provided in the future;
- require that contract guard companies' instructors be certified to teach basic and refresher training courses to guards and evaluate whether a standardized instructor certification process should be implemented; and,
- develop and implement procedures for monthly guard-file reviews to ensure consistency in selecting files and verifying the results.

DHS and FPS agreed with our recommendations.

[17] FPS has approximately 13,500 contract guards, but FPS may review a guard file more than once annually.

[18] For more information on this review and our methodology, see GAO–13–694.

PRELIMINARY RESULTS INDICATE THAT FPS AND SELECT FEDERAL AGENCIES' RISK ASSESSMENT METHODOLOGIES DO NOT ALIGN WITH ISC'S RISK ASSESSMENT STANDARDS

Risk assessments help decision makers identify and evaluate security risks and implement protective measures to mitigate the potential undesirable effects of these risks. ISC's risk assessment standards state that agencies' facility risk assessment methodologies must: Consider all of the undesirable events identified by ISC as possible risks to Federal facilities, and assess the threat, vulnerability, and consequence of specific undesirable events. Preliminary results from our on-going review of 9 Federal agencies' risk assessment methodologies indicate that several agencies, including FPS, do not use a methodology that aligns with ISC's risk assessment standards to assess Federal facilities.[19]

Most commonly, agencies' methodologies are not consistent with ISC's standards because agencies do not assess their facilities' vulnerabilities to specific undesirable events. For example, officials from one agency told us that their vulnerability assessments are based on the total number of protective measures in place at a facility, rather than how vulnerable the facility is to specific undesirable events, such as insider attacks or vehicle bombs. Because agencies' risk assessment methodologies are inconsistent with ISC's risk assessment standards, these agencies may not have a complete understanding of the risks facing approximately 57,000 Federal facilities located around the country—including the 9,600 protected by FPS and several agencies' headquarters facilities.[20]

Moreover, because risk assessments play a critical role in helping agencies tailor protective measures to reflect their facilities' unique circumstances and risks, these agencies may not allocate security resources effectively, i.e., they may provide too much or too little protection at their facilities. Providing more protection at a facility than is needed may result in an unnecessary expenditure of Government resources, while providing too little protection may leave a facility and its occupants vulnerable to attacks. For example, if an agency does not know its facility's potential vulnerabilities to specific undesirable events, it cannot set priorities to mitigate them.

In addition, we reported in 2012 that although Federal agencies pay FPS millions of dollars to assess risk at their facilities, FPS's interim facility assessment tool—the Modified Infrastructure Survey Tool (MIST)—was not consistent with Federal risk assessment standards and had other limitations. Specifically, FPS's risk assessment methodology was inconsistent with ISC's risk assessment standards because it did not assess the consequence of possible undesirable events (i.e., the level, duration, and nature of loss resulting from undesirable events). FPS officials told us that MIST was not designed to assess consequence, and that adding this component would have required additional testing and validation. However, without a risk assessment tool that includes all three components of risk—threat, vulnerability, and consequence—as we have recommended, FPS has limited assurance that facility decision-makers can efficiently and effectively prioritize programs and allocate resources to address existing and potential security risks.[21] Furthermore, because MIST also was not designed to compare risks across facilities, FPS has limited assurance that it prioritizes and mitigates critical risks within the agency's portfolio of more than 9,600 Federal facilities.

This concludes our testimony. We are pleased to answer any questions you, Ranking Member Barber, and Members of the subcommittee might have.

Mr. DUNCAN. Well, I thank you so much, Mr. Goldstein and all the witnesses for your excellent testimony.

Mr. O'Rourke is recognized.

Mr. O'ROURKE. Mr. Chairman, I ask unanimous consent that the gentlewoman from Texas, Ms. Jackson Lee, be allowed to sit and question the witnesses at the hearing's end.

---

[19] ISC's risk assessment standards define "Federal facilities" as Government-leased or -owned facilities in the United States occupied by Federal employees for non-military activities. Aside from intelligence-related exceptions, Executive branch agencies and departments are required to cooperate and comply with ISC's standards, including its risk assessment standards. These standards do not apply to Legislative branch agencies and Federal facilities occupied by military employees.

[21] For example, if an agency's methodology does not consider all the undesirable events identified by ISC, and/or it does not assess all three components of risk (threat, vulnerability, and consequence), then the agency would have an incomplete picture of risk at facilities assessed using this methodology.

[21] FPS agreed with our 2012 recommendation, but has yet to implement it.

Mr. DUNCAN. Without objection, so ordered.

The Chairman will now recognize himself for 5 minutes.

My intent today is, since we do have a small committee, active committee today, is just to allow us to delve into the issue. We are going to try to adhere to the 5-minute rule, but I will allow some leeway, because I do want some questions answered and I want you to have—to feel free to—to really get into the subject, but within reason. So.

What I would like to do is I want to go to the Navy Yard shooting, Director Patterson, first, and ask you a question about how a FPS officer actually engages an active shooter or doesn't engage.

Then I will back up and start delving into the background checks and what we do to make sure this doesn't happen.

I realize that we have a lot of Federal facilities. I also realize that risk assessment is generally looking at keeping someone from breaking into the facility from outside, and this was a unique inside access issue with the Navy Yard shooter.

So, now we have had to think about that sort of thing versus a typical risk assessment of a facility, looking at the entries and exits and the guards, the personnel necessary to secure the premises.

But now we have got a different scenario to think about.

So, according to your response letter to GAO's report, Director Patterson, a protective service officer, or PSO's, actions if unable to visibly see an active shooter, they are dictated by his or her post orders. Although armed, a PSO is not supposed to engage in tactics associated with law enforcement response.

So, could you please explain in further detail what steps a PSO is supposed to take in an active-shooting situation?

Mr. PATTERSON. Yes, sir, I sure can.

Well, first of all, sir, I just want to let you know that our No. 1 priority is the protection of the people in the Federal facility. That is No. 1.

The first—in the event of an active-shooting situation, the first step to be taken by the PSO, because that is our first line of defense, will be to call our megacenter, to allow them to pass that information on to our megacenter. That is where the information is passed that will allow not only that information to be passed to our inspectors, but also to local law enforcement, that there is a situation that is evolving or taking place in that facility.

Mr. DUNCAN. Excuse me, just a second. Will you do that by landline or would that be a radio comm?

Mr. PATTERSON. It will be both, sir. He will do it by landline and then by radio comm.

Mr. DUNCAN. Okay.

Mr. PATTERSON. So that we have a general awareness of what is going on. Then there will be an assessment by that PSO as to what action that he needs to take next.

Our PSOs are trained to take action in emergency situations. Because they are not Federal or State law enforcement officials, they are constrained by—the contractor is constrained by State law as to what he or his company can do in these situations. So that is why we don't have what we call active-shooter training, if you will, where our PSOs will go out and actively pursue an active shooter.

However, if we come across a situation where that PSO is the only individual in that facility and has no reasonable expectation that law enforcement can respond in a reasonably quick manner, then that individual will more than likely take action to limit the damage of the active shooter.

Mr. DUNCAN. Let me ask this, because as you were talking, I am trying to envision—you have an active shooter in a building like the Navy Yard. The PSO hears the shots, understands lives are possibly threatened, picks up the phone, calls his supervisor to try to get permission or at least let them know what is going on, but then try to get permission on how to act beyond his post orders.

Does the same thing with radio comms. Coordination between the PSOs within the facility. While these bureaucratic, seems to me bureaucratic, steps are put in place or being activated, are lives not threatened even further during that? Is there a delay, I guess is what I am asking? Does that put the public safety at risk?

Mr. PATTERSON. Unfortunately, sir, the challenge here is that we don't know what is really happening and neither does the PSO. So he has a responsibility to the people in that area. His responsibility is to ensure that he can get either—keep people from coming into the building or getting people out of the building.

So he has got a job to do right there. In this case, we are hoping, we believe that we are going to have a quick response by either Federal law enforcement, our folks, or by the State and local, if they are in the area. If the situation dictates that we believe that we are in a remote area and we don't think that someone is going to be able to come quickly, then he will take action.

Mr. DUNCAN. Right, and I get that. We had a conversation yesterday with staff about that scenario. The PSO actually securing his entry-door exit, but also making sure that an exit is available for personnel within the building to flee the scene and make sure no one—another active shooter doesn't come in as part of a team. So I get all that.

Mr. PATTERSON. Right.

Mr. DUNCAN. I just want to make sure there is not a delay. You have answered that question fairly well.

So I want to go to Mr. Marshall and ask, if for any reason an individual is deemed a threat, and I know with the Navy Yard shooter, there was some evidence there, but whether it got to the proper person to make that decision is still being investigated. You know, how we miss those signals.

But if an individual is deemed a threat, are you able to deactivate their access credential remotely? Talk me through the process of how their credentials are pulled or their access is denied and limited, if you could.

Mr. MARSHALL. Yes, sir. If derogatory information about an individual reaches us, we will investigate it and we will take the necessary steps to make sure that if that person is deemed a threat after the investigation, we can deactivate their card. Not only their card, but we can also deactivate their access in whatever physical security access system or PACS system that that person has access to.

That can be done remotely, yes, sir.

Mr. DUNCAN. That is on a swipe. But let's talk about maybe a flash pass or some credential that they may have on their persons. I guess at this point an actual supervisor would take that, if it was a termination issue.

If it was an issue where they were going to restrict their access, would they be issued an additional credential, a different color, a different code on there, which I think is important? How would that be handled?

Mr. MARSHALL. No, sir. If derogatory information reached us, and it was deemed to be good information, we would deactivate their card, both their card and also the access system. We would bring them in and read them out, if they had a security clearance, we would read them out.

So they would not only not have access to Classified information any longer, they would also not have access to facilities. An added step that we would take, once we would deactivate their access, we would also do something called a "do not admit". That is a couple of different things. We would go into our personnel security system, which is an enterprise system, and make a notation in their record in the personnel security system that they no longer have a clearance or access to facilities.

We would also notify the buildings or the locations where that person primarily has a mission responsibility, and we would send a flyer with that individual's picture on it and circumstances surrounding that person's removal of access to that facility. So everybody would be notified.

Mr. DUNCAN. Yes. I think this has some implications with how we deal with TSA and access Air Force training Mr. Hudson may get into. Because I think we are looking at the whole scope of access and whatnot.

Just my last question—you told the subcommittee staff at a recent meeting that DHS lacks information on access control systems across the DHS facilities. Headquarters is in the process of compiling this information from its components. But 10 years after the Department's creation, it is unclear to me why DHS headquarters would not know how to access DHS facilities, how that is controlled throughout the Department.

So what is going on now? Is there some sort of uniformity, some sort of activity now to—listen, I go to a lot of Federal buildings here in this city and I know that access to every building is different. Whether they are DHS-coordinated or whether GSA handles that.

So what is going on? Are we looking for uniformity? Are we looking for changes to those systems? If you could just tell me that.

Mr. MARSHALL. Yes, sir. That is exactly what we are doing, Congressman. We are moving towards a federated system.

Obviously, you know DHS is a legacy agency. We are formed of agencies that were already in existence. As a result of that legacy heritage, everybody had their own PACS systems, their own access controls systems, and they are all completely different.

So the first order of business when the Homeland Security Presidential Directive 12 was implemented was to issue the PIV cards. Because there is no sense in changing out all the readers unless everybody had the card to use on the reader.

So that was a heavy lift. We issued over 250,000 PIV cards with the help of the components. Everybody has a PIV card now.

So then the next step, the next phase was to roll out an implementation of these legacy systems and eliminating them altogether. Last fall, I issued a—with the help of my staff—issued a PACS modernization strategy for DHS, which includes headquarters and the eight components. That directed all the components' chief security officers to develop implementation plans on their strategy for switching out the PACS systems and the readers.

They were required to submit implementation plans by early 2013. They all did. Now we are moving towards the roll out, the switching out of the readers.

Headquarters, which I have oversight over, direct oversight over, we have 34 facilities. All 34 facilities have been switched out. We now have HSPD–12 compliant readers in all the headquarters facilities.

FLETC, which is one of our components, it switched out all their facilities. FEMA, which I am happy to say is leading the effort with this, were the first to switch out all their readers.

So we have—we are at various degrees of completion in this whole process. I know ICE has started to switch out their readers. They are at approximately 12 percent of switching out, so they have begun their roll out.

I know TSA has begun their roll out. They are approximately at 12 percent. Citizen Immigration Service, they are right behind TSA and ICE, they are at about 9 percent.

So mostly the larger agencies like CBP and Coast Guard and the Secret Service, to some degree, they are following close behind. But the important thing to know for this committee is that we have already begun that roll out and a lot of the components are looking for funding streams to accelerate the roll out, but we are well on our way.

Mr. DUNCAN. Yes, well, let me just say that I understand the enormity of the number of Federal buildings across the Nation that you are charged with trying to protect. It is going to take a while. But I am glad to see a task force is looking at that.

My final question—you mentioned 3,200 personnel security guards have been trained. Where are they trained? Is that private training and what is the process of certifying that training facility? Or do they go to FLETC? Are they trained by some sort of Governmental agency? Or is it all private?

Mr. MARSHALL. Is that question for me, sir?

Mr. DUNCAN. Yes.

Mr. MARSHALL. Okay.

Mr. DUNCAN. I think you are the one that said 3,200 officers have been trained.

Mr. MARSHALL. That wasn't me, sir.

Mr. DUNCAN. Okay. Was that Director Patterson?

Mr. PATTERSON. I am sorry. What was the context of the question, sir? I am sorry.

Mr. DUNCAN. Well, regardless, how are the contract personnel, the officers, trained? Are they trained at FLETC or are they trained by private contractors? How is that facility certified? I don't care who answers.

Mr. PATTERSON. Yes, sir, I can answer that. Yes. Our 13,000 contracting guards are trained in a couple of ways. One, much of the training is done in-house by the contractor. But second, we also, as FPS, our inspectors also are trained as trainers to go out and provide much of the—some of the training as well.

For instance, firearms training is conducted by the contractor, but overseen by a firearms instructor from FPS. So there is some oversight where they are in fact doing the training. So there are a number of training venues where you have the contractor who is providing the training, but FPS is providing oversight for that training.

Mr. DUNCAN. They are looking at the total curriculum, not just firearms training?

Mr. PATTERSON. Yes, sir. That is exactly—yes, we look across the spectrum. Now, there are some things that we just leave to the contractor. It might be CPR. We probably don't need to be involved in that and a few other things, but for the most part, yes, we do have oversight.

Mr. DUNCAN. Thank you.

The Chairman will recognize Mr. O'Rourke, the acting Ranking Member, for questions.

Mr. O'ROURKE. I want to thank the Chairman again for making today's hearing possible. I recognize that the true Ranking Member has just arrived. I am going to keep my questions brief, and then we will yield this chair to him.

But on this issue of balance, almost each of you mentioned a risk-based approach and trying to balance the costs and benefits both in dollars and security, and what it is we get out of that. So, for Director Patterson, what kind of metrics do you have or what numbers do you use to know whether or not we have struck that right balance?

Then I want to ask a follow-up question on what you are doing to implement some of the recommendations made by the GAO with respect to that. But first, I would like to ask you to respond to that question about balance and how you measure that.

Mr. PATTERSON. Sure. Well, you know, we have over 9,500 Federal facilities that we are responsible for protecting. Of those facilities, there are a large number that are what we call facilities, security level 4, which really are a very high priority. So we have to take a look at how we dedicate resources to those facilities and doing assessments at those facilities over a period of time.

So, we have a metric there that we look at those number of facilities and how often we get to take a look at and use a risk-based method, if you will, for how often we do surveys at those facilities. Currently, we are surveying those facilities, doing security facility security assessments approximately every 3 years at our most sensitive and vulnerable, what we feel to be, high-risk facilities.

But however, we are applying a risk-based model to look at, you know, what are the real vulnerabilities there; what is the threat; and do we really have to continue to expend really scarce resources on doing it every 3 years, or could we extend that out a little bit? So, we do have a metric there to look at and work with the security council at those facilities to look at what is the right mix of service that we provide relative to the assessment process.

Mr. O'ROURKE. Let me ask you a question, sorry to interrupt you.

Mr. PATTERSON. Yes.

Mr. O'ROURKE. You know, on one end of the spectrum, you could pat down every single person who enters a Federal facility; search every square inch of their cars they are driving into a Federal garage. On the other end, you could wave everybody through without taking any precautions. When you have an event like the Navy Yard's shooting, how does that change your assessment? How does that factor into looking at what you are already doing right now? How does that change your procedures and your policies? How does that change what you are willing to spend on it or what you are willing to ask for to be spent on it?

Mr. PATTERSON. Yes, we look at that very carefully. I will tell you, you know, when an individual is given a PIV card, there is a level of trust that the Government says that we are giving to you based upon a background investigation. We still have confidence in that background investigation process until we find out that it is not serving us well. We still think—believe that it has served us well.

So, as far as doing anything that would be beyond, or moving beyond the current process that we utilize to bring people into the building, we are looking at our processes. We are evaluating them, but we think that they still hold true relative to the protection that they provide us based on the background investigation.

Mr. O'ROURKE. Last question. In terms of GAO findings that we weren't assessing risk at a number of Federal facilities; some of the training issues that the Chairman has brought up, do you agree with those conclusions and findings? Is your plan over the coming year to actively address those based on those conclusions reached in that report?

Mr. PATTERSON. Yes, sir. We have been addressing these since 2010. What we are looking at is a multitude of ways that we can approach the myriad of challenges that we have in this area. We are looking at how we leverage technology. We are looking at how we bring on more folks in specialized areas like contract oversight that will help us to better understand what is going on in our contracts.

We are looking at how we refocus the day-to-day efforts of our inspectors to help us better understand how we can move forward in providing a better service to our customers. So yes, sir, we are, but we have been working on this since 2010 and we have still got some ways to go, but I think we are making a lot of progress.

Mr. O'ROURKE. Thank you.

Mr. Chairman, I yield back.

Mr. DUNCAN. I thank the gentleman from Texas, and now recognize the gentleman from North Carolina, the Chairman of the Transportation Security Subcommittee, Mr. Hudson, for 5 minutes.

Mr. HUDSON. Thank you, Mr. Chairman.

I want to thank our panel for being here today. I appreciate your time and expert testimony.

Director Patterson, thank you for your service to our country. One of the statements you made was that PSOs are constrained by State law in terms of what they can do in response to an incident. Can you help me understand that, maybe give me an example of

a State law that would prevent PSOs from engaging an active shooter?

Mr. PATTERSON. Yes, sir. That would be in the use of firearms. They are regulated—the States regulate the way that they—what they can do and the use of their firearms. So, because they are not Federal law enforcement officers, they don't carry the same statutory authority as we do to go in and take charge of searches in certain situations.

So, State laws will dictate whether or not a PSO has the authority to go in and take certain actions that would normally be performed by a law enforcement officer.

Mr. HUDSON. Has there been any analysis of the impacts of that? I assume, you know, there are certain States that we are all aware of that have more strict gun control laws.

Mr. PATTERSON. Right. As a result of the Navy Yard shooting, we are looking at that and working with our contracting office. We are working with the legal folks, as well as internally within DHS to take a look at, is there something that we can do to maybe move beyond where we are now to actually provide our contracting guards active-shooter training so that it will in fact allow them to go out, pursue, and function as a law enforcement officer would?

Mr. HUDSON. I appreciate that.

I guess the follow-up question would be, as you look at, I guess each State has different ways you can respond. I am still concerned, though, that there is not—seems to be widespread-enough active-shooter training for these guards, even if you can't engage with a firearm. It seems like running through scenarios and having training on how to deal with this type of scenario would still be beneficial.

Mr. PATTERSON. Yes, sir. I totally agree. We are doing that. We are looking at what training—we are working with the security companies now to look at, you know, how we can deliver that training and what training would be beneficial to them. Yes, sir, we are doing that.

Mr. HUDSON. Great. I think that is important.

What role did FPS play in the Navy Yard shooting specifically? Could you maybe give us a little more details, sort-of how that played out and what your role was in that incident?

Mr. PATTERSON. Yes, sir. Well, we didn't play an active role. What we did is when we received a notification that in fact there was an active shooter at the Navy Yard, we did recognize at that point—well, first of all, we were part of the incident command center where the District of Columbia, where the Defense Department and other Federal agencies had a command center to more or less—information would pass back and forth. So we put someone there so that we were in full cognizance of what was going on.

We also recognized at that point that we had a Federal facility that was adjacent, the Department of Transportation is adjacent to the Navy Yard.

So we immediately contacted and worked with the Federal folks there, and looked at whether or not we needed to shut down the building and control access, and we did.

So, from that standpoint, what we did was we ensured that we had complete control of the Federal facilities around the Navy

Yard, so that there was no egressor or someone coming in that we—that shouldn't, as well as standing by for any assistance that the folks at the Navy Yard might need.

Eventually, they did call us and ask for some canine support that we provided. So we sent over a couple of our bomb dogs to assist with their activities over there, as they were working—going through the buildings to assess whether or not the shooter had left some explosive devices.

Mr. HUDSON. Thank you.

Mr. Marshall, according to several news reports, radios failed law enforcement once they got inside the facility that day. What has been done or is being done to ensure this problem doesn't exist for Federal Protective Service or other Federal partners?

Is there a radio interoperability issue that we need to be aware of?

Mr. MARSHALL. Well, let me caveat my answer, Congressman, with, first of all, I haven't been briefed on the Navy Yard incident first-hand, so everything I know about what happened there, is anecdotal.

But I—what I can speak on interoperability to some degree: We learned some lessons, obviously, from 9/11, about the inability of the NYPD and FDNY to interoperate during that incident, so much so that it caused a lot of State and local police departments around the United States to address that issue.

In my former agency, I was actually in charge of addressing that issue, going to an 800-megahertz radio system so that we could interoperate with our regional partners and our allied law enforcement agencies.

Specifically to your question, I did hear, second-hand, that there were some interoperability problems at the Navy Yard. I can speak, first-hand, about what actions I have taken with respect to that issue at DHS headquarters.

I am fortunate enough at headquarters to have a cadre of law enforcement officers who are FLETC-trained with full arrest powers. We work in conjunction with the Federal Protective Service and the contract guard force there.

We also have a great relationship with the Metropolitan Police Second District that services the facility on the Nebraska Avenue complex.

So I asked that question right after the Navy Yard. There are some interoperability issues that we are addressing.

The first thing we did was, we have an opportunity to join the regional police mutual aid radio network, also known as PMARS. I first became acquainted with PMARS when I was a U.S. Capitol police officer, back in the 1980s. So the U.S. Capitol Police is a member of that organization.

So I have petitioned the Metropolitan Council of Governments to become a member of the PMARS system. I believe our application will be accepted, and hopefully when that is implemented, we will be able to push a button, or somebody will be able to push a button and everybody can go to a single talk group and be able to address any kind of incident that might occur.

Mr. HUDSON. Appreciate that.

Mr. Chairman, I see I am out of time, so I yield back.

Mr. DUNCAN. I thank the gentleman.

Now, the Chairman will recognize the Ranking Member, the gentleman from Arizona, Mr. Barber. Welcome to the committee hearing. I know you had a mark-up today. As we mentioned earlier, a lot of Members did. But I am glad you were able to make it, and I recognize you for 5 minutes.

Mr. BARBER. Thank you, Mr. Chairman.

Thanks to the witnesses. I am sorry I wasn't here to hear your testimony in person, but I do have a couple questions. They may have been asked and answered, but I would like to explore them.

Let me start, if I could, with Mr. Goldstein.

The question, first of all, is: Based upon your review of the security screening processes at Federal facilities, what is your view of a need for a uniform standard, no matter what the facility, where it is? Do you believe that we need to have that imposed across all Federal facilities?

Mr. GOLDSTEIN. We haven't looked specifically at whether that policy would be beneficial or not. But I can tell you that the variety of systems used throughout the Federal facilities combined with the fact that many officers, contract guard officers have not been fully trained, certainly does not give FPS or the public or workers, Federal employees, assurance that the facilities are well-protected.

Those things combined I think do create problems for the Government.

Mr. BARBER. Well, let me follow up on what you just said about training and the perhaps inadequacy of the training, particularly with the companies under contract to provide security services.

Could you give a couple of examples—you may have already done it in your earlier testimony—of what you found in regard to the training, of deficiencies with the security companies that have been under contract with DHS?

Mr. GOLDSTEIN. Yes, sir. We found in our review, in the report that is being released today, that several contract guard companies that we interviewed did not have any experience with FPS providing them the active-shooter training or the screener training, both of which are required in their contracts.

Mr. BARBER. Having said that, let me ask Mr. Patterson a follow-up question regarding that.

Every contract that the Federal Government lets has expectations, I presume has performance standards. Could you tell us what the expectations and the performance standards are for contractors with regards to training of their personnel?

Mr. PATTERSON. Yes, sir. We have an expectation that every guard who stands post at a magnetometer or X-ray machine will be trained. Period.

Now, there are not X-ray machines and magnetometers at every post. So, there could conceivably be, quite frankly, a number of posts, a number of guards, who aren't necessarily trained on X-ray and magnetometer services who are serving on duty because they are not at one of those posts.

But our expectation is that if you are standing post at an X-ray or magnetometer, you will be trained in that service.

Mr. BARBER. Beyond that, I assume the contracts have some specificity regarding other aspects of training the personnel.

Mr. PATTERSON. Yes, sir. There are about 13 certifications that each PSO must have in order to take a position as a contract guard, from firearms to CPR to, in some cases, magnetometer and X-ray machine, safety, and things of that nature.

Mr. BARBER. So in order to get out in front of a problem that apparently has been identified by the GAO, in other words, finding those companies that have not fully met their commitments under the contract, what can you, what have you been doing proactively to find out where those deficiencies are identified?

What, if any, contract requirements, in terms of any reimbursement to the Federal Government or any potential loss of contract—what happens, first of all, do you find it; second, what happens when you find there is a problem with a contract agency?

Mr. PATTERSON. Yes, sir. There are a number of things that we do. First of all, our inspectors conduct what we call post inspections. That means they go out to the facilities and they talk to the guards and validate through a number of ways their training. They actually—we are required—it is an FPS requirement for us to review at least 10 percent per month of all of the contractor training records for a particular geographic area.

So if we, within a particular FPS region, that regional director is required to go out and review at least 10 percent of those records.

One of the challenges that we have had is that there have been some inconsistencies in the process in which we review those records. So we are getting that together now and figuring out and going about a, or moving forward in a more uniform manner in how we review those records.

Currently, I have directed a—we are conducting a 100 percent audit in four of the regions to take a look at how—and when I say 100 percent, I am talking about 100 percent right now. We are not gonna wait 10 percent, 10 percent, 10 percent. It is 100 percent within the next few months—2 months, within 4 of our regions, so that we can validate and look at what, in fact, our contractors are delivering to us, relative to the training that they say that they are.

So, we are also developing, working with the Department of Homeland Security Science and Technology group a way that we can electronically validate and track this, so that I don't have 600 of my law enforcement guys out trying to track down over 160,000 training records, okay?

It is inefficient and ineffective right now.

So what we are trying to do is better—instead of having to plow through these records every month, to create an electronic system where these records can be folded into the system and then we can review them that way without having to send our folks to physically go and touch each record. Because it takes a lot of time. Quite frankly, the records can change. Records expire, they change. So in effect, when you have got 160,000 records at any given time, some of those records can be out of date, just because they expire over time.

Mr. BARBER. Well, I thank you. My time is up, but I just want to urge you to continue this aggressive action to make sure that everyone is trained to a standard, because that is one way for sure

that we can hope for the protection to be universal across all Federal facilities.

Thank you, Mr. Chairman. I yield back.

Mr. DUNCAN. I thank the gentleman.

The Chairman will now recognize Ms. Jackson Lee, the gentlelady from Texas, for 5 minutes.

Ms. JACKSON LEE. Mr. Chairman, let me thank both you and Mr. Barber for your courtesies and how timely a meeting this is. I thank you so very much.

I hope that the witnesses, let me thank you for your testimony, will view the work of this committee, this subcommittee in particular, but the full committee Chairman and Ranking Member, as partners in excellence. I see this hearing as an attempt for excellence on behalf of the American people.

Certainly, although we know that the jurisdiction of the Navy Yard falls in particular under DOD, and we know that there is a pending investigation, let me just say for the record two things before I pose my questions.

One, I hope that this committee will have another—I know that we had some conversation, a secured briefing on the Navy Yard circumstances. Second, as a Member of Congress, I am always disturbed no matter what administration it is to rebuff members by talking about a pending investigation. We are sworn as officers of this Nation. We take an oath. We take a signed statement on Classified information. But more importantly, that is an easy way to hinder our oversight, which is it is a pending investigation.

Well, a pending investigation could last for eternity. As I reflect on having been here for 9/11, what we discovered and should have been discovered—maybe it should have been discovered preceding the heinous and horrific tragedy if there was the appropriate interaction between the levels of government with the Members of Congress both House and Senate.

So, I hope that the pending investigation of the Navy Yard will either move quickly or that the persons engaged will recognize that we, as Members of Congress, have a responsibility to the American people and those lost souls to be able to provide immediate solutions and resolutions. Which lies in the questioning that I wish to pose and hopefully will have the time to do so, as I thank all of the Members who are here.

One, like the Ranking Member of the full committee, I believe that we should be enormously concerned of the securing of the Federal buildings that are throughout America. You could look at the Navy Yard as a Federal entity. It had a different jurisdiction, but it was penetrated, as was the Fort Hood in my State, which we continue to mourn the loss of military personnel and civilians who should have technically been on the safest place—one of the safest places in America.

So, my question is to follow up on the training of those who protect. I am reminded of the Holocaust Museum, which is I guess semi-private, semi-public, but let me go further into how do we get a handle on training those who are then contracted-out on these Federal buildings? FPS contracts out. How do we get a handle? Is there an inventory of all of these contractors? Is there a set training structure for all of those contractors? One question.

The second question is: Do we do continuous training of these individuals that are hired? I want to say to those in the Mickey Leland Building in Houston and FPS, we respect and thank you for your great service. We want to make it better.

Last, this is a discussion I had with Chairman Duncan. I would like to know from Homeland Security how you would perceive having the responsibility of doing your background check? Do you do your own background check? Could it not be placed under the Office of Management to be able to have control over the contractors that you contract, and also your employees?

It is a simple task. Mr. Chairman, I know that I am down at the limit, but I would ask for the ability for these individuals to answer the question.

Mr. DUNCAN. I will grant a little leeway.

Ms. JACKSON LEE. I thank you.

I haven't told—I will start with the gentleman from GAO, but I would like a response from the interagency and others who jump in on this last question dealing with the background checks.

Mr. GOLDSTEIN. Ma'am, the work we have done that we are presenting to the committee today doesn't actually get into the issue of background checks. It was focused on the training and the certification of the contract guards. So I am not really in a position to answer that.

Ms. JACKSON LEE. Yes, I wasn't asking you that. You answer the question that you are able to do, which is the training of the contractors and how often. I want other members to answer the background checks question. Thank you.

Mr. GOLDSTEIN. Certainly.

We do feel that more attention to training and certification on the part of FPS is required. Much of the training that the contract guard companies say they are not getting is training related to active shooters and to other screening that is presented by FPS.

To some degree, there has been an issue of shortages among personnel to get out to all the contractors, but to be fair, they have had a number of years. We first raised the issue of screener training about 4 years ago when we did penetration testing at Federal facilities around the country and were able to get bomb-making materials into 10 Federal buildings in 4 cities.

So this has been an open issue now for a number of years. So, to still have Federal Protective Service contract guards at Federal facilities who don't have the required training to be in front of the machines they are using, this does not bode well.

Ms. JACKSON LEE. Again, the rest of the members there, answer the question about do you do your internal background checks, do you continuously have background checks on your contractors? Do you believe with a structural change, maybe the collaboration of this committee to internalize the background checks on both contractors and on your own staff for homeland security?

Mr. MARSHALL. Yes, ma'am, I can answer that question.

Everybody who works for the Department of Homeland Security, both the Federal employee or contract employee, has to have either a suitability determination or a fitness determination. Essentially what that is is that even though they are called two different things, the criteria is the same. We are trying to determine if that

person belongs in DHS and is suitable for employment, and is in the best interest of the agency and for the efficiency of Government.

We look at things like conduct in past employment, criminal history, alcohol and drug abuse, that type of thing; whether or not the person has engaged in any activities that are contrary to U.S. interests and so forth.

With respect to contractors, they undergo the fitness. We, DHS, we adjudicate for that fitness determination. If that contractor has to have a security clearance, a National security clearance, that is conducted by the Department of Defense, Defense Security Service. They have jurisdiction over those investigations under the National Industrial Security Program.

So, we do the fitness and we do the adjudication for the fitness to determine if that person is suitable, but any kind of security clearance falls under the purview of the Department of Defense.

Ms. JACKSON LEE. So after you do your clearance, if they do not need a National security clearance, that person is hired.

Mr. MARSHALL. Correct.

Ms. JACKSON LEE. Do you do it for the contractors as well?

Mr. MARSHALL. Yes, ma'am. That is correct. If there is no derogatory information developed, that person is deemed to be suitable to enter on duty and they can come on-board.

Ms. JACKSON LEE. May I ask Ms. Durkovich, you were tasked by President Clinton to—the agency was tasked to set certain standards for Federal buildings. Where is that in terms of its implementation and oversight of the security of Federal buildings throughout the Nation, I assume, working on the security protocols for all of the Federal buildings?

Ms. DURKOVICH. Thank you. That is a very good question, Congresswoman.

We have been hard at work for the last 17 years working with our 53 member agencies to develop a set of physical security criteria that is included in our risk-management process for Federal facilities. This is applicable to 399,000 non-military Federal buildings across the United States. Our member companies—our member organizations are responsible for developing these standards.

Our risk-based process for Federal facility standards includes six key elements, the first of which is establishing the Federal security level for a building. That is driven by the function of that particular building, the agencies that reside in it, the people who pass through it, the iconic and historical significance of that building.

Once that physical security level is set, we look at the baseline standards and measures and mitigation measures that are applicable to that building, and then look at 31 different, what we call design basis threat scenarios. So it ranges from active-shooter scenarios to arson to water to small aircraft. Based on those scenarios and physical—the facility security level, the facility is responsible for implementing the physical security criteria.

All of the member agencies, according to the Executive Order, shall comply with the standards that they develop. So I would say over the course of the last 17 years, we have been very successful in helping implement a baseline security standard for non-military Federal facilities.

Ms. JACKSON LEE. What is the oversight? Who is checking?

Ms. DURKOVICH. At this juncture, we do not have the resources to do formal compliance. Many of our member agencies have developed risk assessment tools that allow them to ensure that they are in compliance with these standards.

We are looking at ways to begin more of a soft compliance effort, but again, the Executive Order requires our member agencies to comply with the standards that this interagency body develops.

Mr. DUNCAN. Ms. Jackson Lee, we may have time for another round of questions. So I——

Ms. JACKSON LEE. But can I just thank you very much for your courtesies? I would just like to put one question on the record. I will not ask for an answer. I didn't hear from Mr. Patterson. That one question on the record, if we could get an answer, is: Does FPS do—FPS, does it do continuing background checks on its contractors once the contract is given? Is there an on-going check on the individuals that are utilized?

Mr. Chairman, Mr. Barber, thank you for your courtesy.

Mr. DUNCAN. Thank you, Ms. Jackson Lee.

That is a question we can have answered.

I am going to go into a second round of questioning. I know Members do have a lot of interest in this subject, including myself.

I want to follow up on—I recognize myself for 5 minutes—I want to follow up on an issue that Mr. Hudson brought up about the radios, because I think that is important, communications inside of a building and communication with local law enforcement is tremendously important.

In my State, the Palmetto State, South Carolina, we learned after Hurricane Hugo that law enforcement needs to be able to communicate all across the State. I believe with a homeland security grant back after 9/11, the State of South Carolina went to an 800-megahertz radio system that we had highway patrol and DNR, and local sheriffs' agencies were all able to communicate in the event of an emergency.

I understand that inside the District of Columbia, FPS may not want to hear all the chatter that is going on on the Hill and at the White House and at every other Federal building. That could be a little overwhelming if you were having to monitor all of that. But in the event of an active shooter, can they communicate with other law enforcement personnel about what is actually going on?

So I am going to ask Mr. Marshall if you could just follow up on that. What are we doing? What steps are we taking to address the issue raised by the gentleman from North Carolina?

Mr. MARSHALL. Congressman, I would like nothing better than to have an 800-megahertz radio capability within DHS. Speaking first-hand, like I said, I have implemented that in the local police department here in Maryland, a neighboring police department. The capabilities are tremendous with an 800-megahertz radio system.

You don't have to listen to, like you said, all the chatter at the Federal buildings and so forth. But in the event of an active shooter, you would be notified to go to a specific talk group, everybody involved in that incident, say. Let's use the DHS headquarters, for example, on Nebraska Avenue. If, God forbid, something were to

happen at DHS headquarters, we can notify our colleagues at the Federal Protective Service, Metropolitan Police Second District, my force protection group, to all go to a specific talk group to handle that incident.

You are absolutely right. That capability is vital in any kind of incident.

Mr. DUNCAN. Would something like an 800-megahertz system be able to penetrate most of the walls so most of the Federal facilities would be able to communicate?

Mr. MARSHALL. Yes, sir. In my experience now, obviously, we would have to do something called acceptance testing. We would have to—once we were able to acquire that capability, we would have to go to certain spots on a grid and test the radio to find out where those dead spots might be. But from my experience, it works in like 99 percent of the locations, at least where I came from.

But again, that capability is vital. So if that is available, I know those 800-megahertz frequencies are like hen's teeth. They are hard to get your hands on, because I think most of them are taken up. But I believe the Metropolitan Police is on an 800-megahertz system. If for some reason we could—or some, you know, capability to attach ourselves to the Metropolitan Police or, for that matter, Federal Protective Service or any other Federal Government agency who has that 800-megahertz frequency, that would be the ideal situation in the District of Columbia.

Mr. DUNCAN. Right. Well, thanks for that. I may have taken Mr. Hudson's question, but it was on my mind.

I want to ask you one other thing. Mr. Marshall, what have we learned about background checks and information flow that would affect clearances like we saw with the Navy Yard shooter, where local law enforcement, even supervisory positions within the agency they worked for, they had indicators?

So how does that—what have we learned? How does that information flow down to the person that makes the decision on who gets clearances or not? Just tell me what we have learned and how we are applying it.

Mr. MARSHALL. Okay. First of all, you mentioned the local agencies. One of the things I have always been troubled with with respect to local agencies is that there are roughly between 18,000 and 20,000 police departments or law enforcement agencies, sheriffs, local police, State police, and Federal agencies within the United States.

The thing that has troubled me about what, the information we receive from the State and locals and the Federals, is that not all of those agencies contribute to, like, the FBI CJIS system. A person can be arrested in your State, the Palmetto State, and some small police department. They may not be a contributor to the FBI database. So that when we go to do our agency checks and our fingerprint checks, we may not have access to that information of that person's arrest within South Carolina.

So, that is a gap. That is a gap that I think can be remedied. I don't know what it would take, maybe legislation perhaps, but that if we can get more of these agencies—and I don't know what percentage that are out there that don't contribute. But I believe it is large enough that we could probably close that gap somewhat

by maybe encouraging, legislating for these folks to contribute, particularly if they get Homeland Security money.

Now, with respect to the second part of your question, again, I wasn't briefed on the Navy Yard shooting specifically. But what I know through the media accounts and some anecdotal comments or conversations I have had with other people, from what I know, Mr. Alexis had a security clearance with the Navy. When he left the Navy, it was still an in-scope clearance, meaning that the investigation was within the required time frame in order for the organization he was going to to accept that investigation on reciprocity.

We are required by Executive Order in the Federal Government to accept security clearances on reciprocity if there is an investigation that we can point to. The one thing about reciprocity is that we are also required to accept it on its face. We are not allowed to do any additional checks unless we have information—derogatory information to the contrary.

So, it looks to me, not having been briefed, that the contracting company accepted Mr. Alexis's security clearance on reciprocity, which was one gap, without having to do additional checks. That also there was a faulty investigation. There was information within the investigation that was done by a private contractor that wasn't accurate.

So, it was almost like a perfect storm. It was a gap that was—it was unfortunately hard to overcome.

Mr. DUNCAN. Yes, we are human. I get that.

Mr. MARSHALL. Yes, sir.

Mr. DUNCAN. Timing is everything. So, I don't have any further questions. I will ask the gentleman from North Carolina if he would like to follow up with a 5-minute question.

Mr. HUDSON. Thank you, Mr. Chairman.

I guess I would like to maybe get back to this issue of communications between, you know, FPS and the local and State agencies. Mr. Marshall mentioned there are 18,000 to 20,000 law enforcement agencies around the United States.

In terms of passing along warnings, intelligence, information about suspects, could you, Mr. Marshall, and also Director Patterson answer if you like, maybe talk about what the gaps are that exist there, whether it is information flow from DHS down or from local law enforcements up, FPS, back and forth.

What are the gaps in communications? What are the real challenges?

I know some were highlighted with the Boston bombing incident, others may—we may have learned lessons from the Navy Yard. But what are some of the challenges we are facing when it comes to that up-and-down communication?

Mr. MARSHALL. Well, Congressman, we are very fortunate in the Washington, DC, area to have so many law enforcement agencies, both Federal and local, and, of course, the regional county police departments.

We are all members of that fraternity here, within this region. I believe we communicate very well together. We are all part of different working groups and organizations, intelligence organizations.

So, I believe our sharing capability is a good one here, within this region.

Where I have seen some gaps during my time here is when you get outside of this D.C. area and you deal with people who are coming in from other parts of the country. We don't always communicate well in that regard.

We rely heavily on information from the criminal justice information system. If we see somebody suspicious, obviously, we would rely on a radio check for, you know, a criminal history check or a radio check, wants and wanted type of BOLOs and so forth.

But regionally, I think we are okay. It is when we get outside of this region where I don't think we share often as well as we should.

Mr. HUDSON. Director Patterson.

Mr. PATTERSON. Yes, sir. I would agree with Mr. Marshall that within the region here, I think we do a pretty good job.

Part of the challenges that we have in FPS is that, as you well know, we are in 50 States. Some of our inspectors have to travel a very long way to move from facility to facility, sometimes between States.

The challenge there sometimes is that the radio—the connectivity that they have when they leave one State to go to another State, we lose it.

So we have to work within those States or with other Federal agencies to try to help us bridge between the facilities, sometimes, that our inspectors may travel.

On the intelligence side of things, though, I think we do pretty well, because we try to link up with each one of the States' fusion centers, as many as we can. We have people that are linked and members of the joint terrorism task forces.

So relative to threat information and those kind of things, we think we move that information fairly well up and down and have pretty good access.

It is sometimes—what concerns me sometimes is just the ability and officer safety issue of, can my officer or can my inspector communicate or call for help if, in fact, he runs into a problem, if he is maybe somewhere in the northern tier, where it is—he is right out in the middle of nowhere and help is a bit of ways away, and he has got to figure out which radio he is or how he is gonna communicate back to ask for help?

We are working that. We are working within the Department, and we are working with State and local as well as other Federal agencies, again, to bridge those gaps where we recognize them.

Mr. HUDSON. Appreciate that. Obviously I think this committee is very concerned about this issue, so please keep us informed as you move forward with this.

Just to sort-of redirect a little bit, Ms. Durkovich, you talked a little bit about sort-of different facilities that are leased or owned by GSA and the different security level depending on the type of facility.

You talked about the fact that ISC has set security standard guidelines for these non-Federal—or non-military Federal facilities.

How well does the Federal Protective Service, in your opinion, follow these policies? Does their adherence differ based on the different type of location of the Federal facilities?

Ms. DURKOVICH. Let me begin—and, first of all, thank you very much for that question—but by saying that FPS is an active member of the Interagency Security Committee.

We have worked over the course of the last several years, both at—within the Office of Infrastructure Protection, but certainly with—within ISC to help them understand and implement the various standards, guidelines, and practices that we develop. Certainly, as they have worked to develop their own assessment tool, it has been done with the ISC standards in mind.

I would say that they do a very good job. Again, it varies on the facility security level and the measures that are implemented at each of those facilities. But they have to work very closely with the facility security committee within each of those buildings to ensure that they are providing a level of security that is consistent with the Federal security level and the standards that are outlined by the ISC.

They are, again, a very active participant in the ISC. They sit on a number of our standing committees, on a number of our working groups, to include the active-shooter working group. They recently chaired a working group on prohibited Federal items, which has become a standard for Federal facilities across the Nation, and have worked very closely with us with some best practices on armed security guards.

So they are an active, robust member, again of the ISC, and I think do a very good job of implementing the standards and best practices that we promulgate.

Mr. HUDSON. Thank you.

Mr. Chairman, thanks for the leeway. I will yield back.

Mr. DUNCAN. Thank you, Mr. Hudson.

The Chairman will recognize the Ranking Member for the last and final questions.

Mr. BARBER. Thank you, Mr. Chairman.

Once again, thanks to our witnesses this morning for your testimony and for the work you are doing to make sure that Federal facilities, the people who work in them, and the people who come to them are properly protected.

I just wanted to continue with a question for Mr. Patterson regarding what you are doing proactively, I guess, to probe and test how well safety and security standards are being implemented.

Within the context of this open hearing, you may not be able to say all, but what can you tell us about what you are doing proactively to find out whether or not these facilities are following the standards that have been established?

What do you do when you find that they are not?

Mr. PATTERSON. Sir. Yes, sir.

Well, one of the things that we are doing proactively is that we are creating something called a portfolio approach for each one of our inspectors. That means that the inspector will take ownership of a series of buildings, okay, and within those buildings will have responsibility to ensure that he or she are meeting with the facility security committees and others in there to ensure that we are, No.

1, in compliance or that they are in compliance with whatever standards that have been set forth for that facility.

So that is a very proactive approach by us to ensure that we don't miss anything in a movement forward to better understand how we can, if you will, better do our job.

We are working with the NASCO, the National Association of Security Companies, in looking at how we can collaborate, how we can partner in working in training our PSOs, relative to giving them the best training, better training, and to fill in the gaps that were pointed to today by the General Accounting Office, so that the next time that we come before this committee, we are not talking about some of the challenges that we are having there, because we have, in fact, taken a proactive approach in filling that, because we are working collaboratively with the security companies.

We are also looking at partnering with local law enforcement in areas, departments, to help us in our response times, to ensure that when there are challenges for our inspectors to get to Federal facilities, that we do have an agreement and a partnership with them that they will respond sometimes when we cannot.

So there are a myriad of things that we are looking for as moving forward to ensure that we have a very comprehensive approach to how the people, which are the most important thing, are protected in those facilities in the event of something bad, if you will.

Mr. BARBER. Does your proactive work include deliberately trying to breach these securities?

Mr. PATTERSON. Yes, sir, we have a program called the covert testing program, where we actually have—we have a number of scenarios that we introduce through the system when we, through the magnetometer, X-ray, and it is done by our special agents, who are trained in introducing these objects.

Once—you know, if there is a failure, then what we do is we work with the contractor to, No. 1, that we have identified a failure. Then we work to train those individuals so that there is an understanding of what just happened, what did we just do? How do we fix this? How do we rectify the situation so that it doesn't happen again?

Sometimes we have to do it more than once, quite frankly, to—it is the process of standing behind a magnetometer X-ray machine, it can be a perishable skill if you are not doing it often.

So one of the things that we are doing proactively is to work with the contractors to look at, you know, how often this training is being delivered to them? Then we are gonna look at how often we are testing that, and then using a metric there to see how well we are performing in that area.

Mr. BARBER. Let me just ask you one last question before my time expires.

Mr. PATTERSON. Sure.

Mr. BARBER. Obviously, every Federal agency has been asked to not only tighten their belt but cinch it up so tight you can hardly breathe.

What impact have budget cuts or appropriation reductions had on your ability to get the job done?

Mr. PATTERSON. We are still able to get the job done, sir. You know, we have to work smarter. We look to how we leverage tech-

nology to do things that maybe we had done using an individual, and now—so, we are getting the job done, even with the sequestration and some of the budget cuts that have been coming. I am confident that we will continue to be able to effectively get the job done as we move forward.

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

Mr. DUNCAN. I want to thank the committee Members for their participation today, and thank the witnesses. As we mentioned, I think the goal of the hearing was to provide oversight of the DHS, and what it is currently doing to make sure that we protect Federal facilities, and what steps, if any, need to be taken to make sure that instances like the Navy Yard don't happen at any other Federal facilities.

I want to thank you for your leadership and your valuable testimony today. You answered a lot of questions for us as we delved into that. So I want to thank you for that, and the Members for their valuable questions.

Members of the subcommittee may have additional questions. We ask that you respond to those in writing.

Without objection—any other questions, or without objection, the subcommittee will stand adjourned.

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

APPENDIX

QUESTION FROM CHAIRMAN JEFF DUNCAN FOR L. ERIC PATTERSON

Question. What is the status of the standardized National Lesson Plan for guards, and the revising of the Security Guard Information Manual (SGIM)?

When will the National Lesson Plan for guards be implemented?

Answer. The Federal Protective Service (FPS) recognizes that ensuring that Protective Security Officers receive quality training is key to the success of the FPS protective mission. As such, FPS is working with the National Association of Security Companies (NASCO) to conduct a curriculum review of all Protective Security Officer (PSO) training. This review will consider long-standing requirements pertaining to PSO training and will result in a comprehensive PSO basic training curricula complete with written and performance measures. FPS anticipates that the PSO National Lesson Plan will be finalized and available for implemention in fiscal year 2015. The Security Guard Information Manual (SGIM) is undergoing a complete revision and will be released as the FPS Protective Security Officer Security Manager and Resource Tool (SMART) Book. An updated version of the SMART Book is expected to be released by the end of the second quarter of fiscal year 2014.

QUESTIONS FROM RANKING MEMBER RON BARBER FOR L. ERIC PATTERSON

Question 1. Does FPS conduct on-going evaluations of both its contract guards and Federal workforce?

Answer. The Federal Protective Service (FPS) conducts rigorous and continuous Protective Security Officer (PSO) contract performance monitoring through various methods, including post inspections, administrative audits, monitoring of contractor-provided training and firearms qualifications, penetration tests, and obtaining customer feedback. FPS adheres to policies and procedures to ensure proper contract monitoring, including FPS Directive 15.9.1.3 "Contract Protective Security Force Performance Monitoring" and Office of Procurement Operations (OPO) Procurement Operating Procedure (POP) 403R4 "Contractor Performance Assessment Reporting and Procedure".

FPS Contracting Officers have the ability and authority to take contractual actions to address contractor performance that does not comply with contract terms and conditions. Specifically, FPS employs remedies available under the Federal Acquisition Regulations and within the terms of its contracts to address contractor performance issues. A number of remedies are available for a contractor's non-performance or unacceptable performance in FPS PSO contracts. Remedies include, but are not limited to monitoring of contractor corrective action plans, assessing monetary deductions, directing removal of a contractor employee from performing under a contract, electing not to exercise a contract option, or terminating a contract for default or cause.

To ensure robust contractor oversight, FPS is currently in the process of hiring and training 39 Contracting Officer Representatives (COR). CORs will assist FPS Contracting Officers in identifying adverse contract performance and taking timely corrective action.

FPS adheres to the performance management regulations established by the Office of Personnel Management, and guidelines of the Department of Homeland Security and National Protection Programs Directorate to evaluate Federal employee performance.

Question 2. Mr. Patterson, what protocols are used by FPS' facility security officers and facility security committee members to determine which standards to implement at Federal facilities?

Answer. The Federal Protective Service (FPS) provides Facility Security Committee members with recommendations as part of the FPS's Facility Security Assessment (FSA) process. FPS designed its FSA process to meet the requirements of

the Interagency Security Committee's (ISC) Risk Management Process for Federal Facilities. The FSA report provided by FPS includes an assessment of threats and vulnerabilities, and a comparison of the baseline level of protection called for in the ISC process with the existing level of protection at the facility, and FPS's recommendations for countermeasures to mitigate risk.

FPS has also established an FSA steering committee to ensure consistency in implementation of the FSA program. The primary mission of the Steering Committee is the coordination of all FSA-related standards, programs, and operational applications. The Steering Committee serves as the FSA consultation entity, providing clarification and updates on development of the FPS FSA program. The Steering Committee also assists FPS Regions with guidance on the implementation of FSA reports, policies, and applications.

Question 3. How does FPS intend to address the shortcomings of its risk assessment methodology as identified by GAO, particularly its absence of a component to assess consequence?

Answer. The Federal Protective Service (FPS) has incorporated the Interagency Security Committee's (ISC) Risk Management Process for Federal Facilities into its current Facility Security Assessment (FSA) process. Specifically, the FSA process includes the ISC's Facility Security Level (FSL) Determinations, Physical Security Criteria for Federal Facilities, and the Design Basis Threat as incorporated into the Modified Infrastructure Survey Tool to identify and mitigate vulnerabilities. FPS also conducts a threat assessment and provides a Threat Assessment Report as part of each FSA, to ensure that stakeholders have an understanding of the threats they face.

While potential impacts are considered as part of the FSL determination, FPS is continuing to explore the inclusion of consequence into the process. Quantifying applicable categories of consequence for Federal facilities and incorporating them into an algorithm in an assessment tool, however, is currently not feasible as there is not a body of work existing to facilitate such development. FPS continues to work with the ISC to explore consequences and impacts in the context of Federal facilities and missions.

Question 4a. FPS has a long history of budget woes due to its reliance on fees, and a workforce that has too many contract guard staff. Further, GAO has documented that FPS' contract guard staff has been about 13,000 since 2001.

What is the current ratio of contract guard to Federal guard staff at FPS?

Question 4b. What elements are contained in FPS' contracts pertaining to the training curriculum used by private firms to train and certify guards?

Answer. To accomplish its protective mission, the Federal Protective Service (FPS) employs Law Enforcement Personnel as well as contract Protective Security Officers (PSOs) who work in tandem to attend to daily security needs at Federal facilities and respond to threats directed against the facilities or the personnel working within them. Law Enforcement Personnel and PSOs have separate, but complementary, roles and responsibilities in ensuring Federal facility security.

FPS directly employs approximately 1,007 Law Enforcement Personnel who are trained physical security experts and sworn law enforcement officers employed directly by the Federal Government. Law Enforcement Personnel perform a variety of critical functions, including conducting comprehensive security assessments of vulnerabilities at facilities, developing and implementing protective countermeasures, and providing uniformed police response and investigative follow-up. FPS Law Enforcement Personnel also conduct PSO guard post inspections on a daily basis.

FPS also contracts approximately 13,000 PSOs, often referred to as "security guards." PSOs are responsible for controlling access to Federal facilities, detecting and reporting criminal activities, and responding to emergency situations.

PSOs also ensure prohibited items, such as firearms, explosives, knives, and other dangerous weapons, do not enter Federal facilities. It is important to note that PSOs are not sworn Law Enforcement officers. FPS works with the private guard companies to ensure the guards have met the certification, training, and qualification requirements specified in the contracts. These include, but are not limited to, FPS orientation, National Weapons Detection training, weapons qualification for both lethal and non-lethal weapons, FPS Basic Training, which covers subject areas such as defensive tactics, legal authorities, and response to incidents such as workplace violence, and bomb threats, and any State, local, and customer-specific requirements.

It is important to note that the FPS does not unilaterally determine the total number of PSOs Nationally. Rather, the FPS works in partnership with tenant Facility Security Committees to build a consensus regarding the number of guard posts appropriate for each individual facility. The number of posts is determined by a

number of factors, including a facility's security level, Facility Security Assessment, and the security needs and preferences of tenant agencies.

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR CAITLIN DURKOVICH

Question 1. Ms. Durkovich, in your role as chair of the Interagency Security Committee, what steps are you taking to make sure that Federal agencies are compliant in utilizing the committee's standards for physical security?

Answer. Executive Order (EO) 12977 states that each executive agency and department shall cooperate and comply with the policies and recommendations of the Interagency Security Committee (ISC) issued pursuant to the order, but at this time the committee does not have the resources to carry out enforcement for nearly 400,000 facilities Nation-wide. The ISC relies on agencies to conduct their own compliance as required by the EO.

That said, the ISC is examining potential options to support agencies' compliance efforts and is currently reviewing internal member agencies' best practices and lessons learned to develop a strategy to propose to the ISC membership. This work is being conducted through the ISC's Lessons Learned and Best Practices Working Group; a group established as a result of Government Accountability Office (GAO) Recommendation Report GAO 12–901 *Federal Real Property Security—Interagency Security Committee Should Implement a Lessons Learned Process.*

Additionally, the ISC has also developed a strategy for Federal departments and agencies to ensure risk assessment data tools are compliant with ISC standards. To date, one tool has been certified as ISC compliant and another tool is in the queue for certification.

Question 2. Please explain the actions your staff is taking to increase the rate of utilization of the committee's standards.

Answer. The ISC is developing an outreach strategy to improve engagement, marketing, and training efforts. The plan defines the goals and objectives of future outreach efforts; specifies the target audience of outreach activities; and describes outreach options. This strategy also consists of a number of on-line training programs, personal interaction, printed materials, and on-line communications.

The ISC currently relies on Chief Security Officers (CSOs) and working group representatives to share information about ISC standards and best practices. The ISC is developing an enhanced outreach plan to increase awareness and improve marketing and training efforts. The plan will increase marketing activities, providing CSOs with materials they can share with their facilities, as well as new on-line training programs, on-line communications, and greater personal interaction.

Question 3. How do you evaluate the outcomes of your agency's outreach efforts in terms of measuring Federal agencies' usage of the Interagency Security Committee's standards?

Answer. As noted above, the ISC is currently assessing and enhancing its outreach efforts. The Interagency Security Committee Outreach Strategic Plan will provide a foundation for the ISC's implementation of outreach activities to increase awareness, understanding, and use of the ISC Standards, guidelines, best practices, and white papers among Federal agencies. The ISC developed a plan that defines the goals and objectives of future outreach efforts; specifies target audiences; and describes three categories of outreach options: Printed materials, personal interaction, and on-line communications which is consistent with the GAO's recommendations. An important aspect of the ISC's outreach is training and the ISC is currently doubling training available to Federal agencies. Both on-line and in-person training will be amplified through implementation of the plan. The implementation of the outreach plan will enable the ISC to better measure the most effective and efficient approach for increasing awareness, understanding, and application of the ISC standards.

QUESTION FROM CHAIRMAN JEFF DUNCAN FOR GREG MARSHALL

Question. During the October 30 hearing, you discussed remotely deactivating access credentials if a change in an individual's suitability occurs. To clarify, how long does the deactivation process take? Can it be done in real time to avoid potential threat?

Answer. The deactivation process can be done in real time and from remote locations. Execution of this access removal process includes the revocation of the individual's Personal Identification Verification Card (PIV card) in the Identity Management System (IDMS), suspension of access in the electronic physical access control system (PACS) that services the component who employs the individual, and updates to security guard post orders to include "Do Not Admit" instructions associated with the individual. Manual notifications are provided via email and/or tele-

phone to all respective organizational points of contact to support facilities where either visual inspection or electronic verification is performed. Automated PIV card revocation checks is a functionality that is supported by the IDMS. DHS is currently working to deploy this capability to all the components.

QUESTIONS FROM RANKING MEMBER RON BARBER FOR GREG MARSHALL

Question 1. Mr. Marshall, please explain to the committee what standards are involved in granting individuals' access to Federal facilities. Also, what process is used to identify and individual as being suitable for Federal employment?

Question 2. Also, please describe to the committee how the mental health of an individual is taken into consideration when making a determination about his or her suitability for Federal employment?

Answer. All individuals working for or on behalf of the DHS must undergo a background investigation with favorable results. In order for an individual to gain access to a DHS facility, a criminal history check with favorable results must be completed. For issuance of a PIV card, the background investigation must be initiated in accordance with Homeland Security Presidential Directive 12 requirements.

DHS adheres to all Federal regulations and guidelines for suitability for Federal employment. DHS uses the criteria set forth in 5 Code of Federal Regulations, Part 731, to assess an individual's suitability. The individual completes security paperwork, Standard Form (SF) 85P, and undergoes a background investigation. Based on the suitability criteria, an adjudicative determination is made whether the individual will promote the integrity and efficiency of the service.

Currently, there are no requirements for individuals to report mental health information when applying for Federal employment for non-cleared positions; however, OPM does permit agencies to use the SF 85P–S supplemental form for positions that require the carrying of a firearm. This supplemental questionnaire does require individuals to report consultation with mental health professionals and/or health care providers regarding a mental health condition. Otherwise, when DHS adjudicates a background investigation, the mental health condition of an individual is only considered to determine eligibility for access to National security information. It is reviewed when the individual chooses to report this information on standard security form SF–86, or during investigative interviews and other records checks. In cases where mental health information is not reported in an investigation by the individual, references, or by review of records, potential mental health issues are not examined. This poses a vulnerability and risk to the Department.

In National security clearance investigations, DHS can obtain mental health records when the information is reported either on the security forms or through investigative interviews. This is in accordance with Executive Order 12968, Access to Classified Information and its implementing guidance. Additionally, the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information requires DHS to evaluate an individual's ability to handle and protect National security information. DHS renders adjudicative determinations for access to classified material.

When evaluating the information, DHS must apply the adjudicative criteria, which includes evaluating whether an individual's mental health condition adversely affects the individual's judgment and trustworthiness to safeguard classified information.

Question 3. Mr. Marshall, what authority and access do you as a security professional have to the mental health records of individuals seeking approval for access into Government facilities, or to be cleared for Federal employment?

Answer. As a security professional, I do not have categorical access to mental health records for the approval of access into DHS facilities or to be cleared (suitable) for Federal employment. In National security clearance investigations, DHS can only obtain mental health records when the information is reported either on security forms or through investigative interviews, and then only with the consent of the individual being investigated and the cooperation of the provider. At DHS, when applicants submit their security forms, included in their packages are signed release forms that allow investigators the ability to pursue information reported by the applicants on their SF 86 or other security/suitability questionnaire. The applicant's signature signals "consent" and the intent of the applicant for mental health providers to "cooperate" with any investigation. This is in accordance with Executive Orders and implementing guidance.

Question 4. With regard to suitability assessments, does the Department contract with private firms to conduct background checks? If so, who is responsible for vetting contractors who conduct the checks?

Answer. Yes, the Department does contract with private firms to conduct background checks. The Office of Personnel Management and the Department of Defense have oversight responsibility for the background investigation contract workforce. OPM delegates investigative authority to certain DHS components, who then employ contract background investigators. It is a requirement of the delegation that contract investigators must have been appropriately adjudicated. The Department of Defense has responsibilities regarding the security clearance adjudications of contract employees under the National Industrial Security Program. DHS accepts reciprocity of the investigation and adjudication of contract background investigators.

QUESTIONS FROM CHAIRMAN JEFF DUNCAN FOR MARK GOLDSTEIN

Question 1. Your testimony noted that taxpayer dollars may be put at risk because of problems with FPS's risk assessment process. Specifically, you said that these problems may result in facilities with too much or too little protection.

On this issue, I think back to earlier in the year when many were alarmed by FPS's presence at protests outside IRS buildings. How does the risk assessment process impact FPS's responses to specific events, such as peaceful protests?

Answer. Risk assessments, which are among FPS's physical security responsibilities, allow FPS to determine which protective measures should be in place at a facility. Responding to events/incidents, such as peaceful protests, is among FPS's law enforcement responsibilities. While the risk assessment process does not directly influence how FPS responds to specific events, it allows FPS to determine whether and what types of protective measures are needed to help mitigate the risks associated with these events.

Question 2. How does the fact that FPS collects fees for certain services impact the oversight performed by DHS? Do you think because FPS collects fees for certain security services that less oversight is conducted by DHS than if the programs were based on appropriations?

Answer. We have not conducted the work necessary to answer this question. For information on FPS's fee design, proposed alternatives, and challenges related to FPS and customer agency budget formulation, please see GAO's May 2011 report *Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security* (GAO–11–492).

QUESTIONS FROM RANKING MEMBER RON BARBER FOR MARK GOLDSTEIN

Question 1. Mr. Goldstein, is there a need to impose a uniform physical security screening standard across the Federal Government? Also, should the Capitol Hill standard of administering a full screening of all personnel and visitors to Federal facilities regardless of their security clearance status be adopted?

Answer. We have not conducted the work necessary to answer this question.

Question 2. What process do agencies and departments use to determine which physical screening standards to apply throughout the Federal Government?

Answer. To determine which physical screening measures to implement at Federal facilities, Federal agencies generally conduct risk assessments. These assessments evaluate the threat, vulnerability, and consequence of undesirable events (such as terrorist attacks or other acts of violence) occurring at a facility. After the assessments are completed, the information is used to determine risk and to recommend countermeasures, such as physical screening measures, to mitigate it.